LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 44/2003
/V

Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve

Liikenne- ja viestintäministeriö
Helsinki, 2003

Esipuhe

Ajatus selvittää sähköisen tunnistamisen ja teknisen valvonnan menetelmiin liittyviä ilmiöitä herätettiin liikenne- ja viestintäministeriössä keväällä 2003 sähköisen viestinnän tietosuojalain valmistelutyön yhteydessä.

Tietoyhteiskunnan kehityksen myötä oli nähtävissä ajankohtainen tarve rohkaista sähköisten tunnistusmenetelmien kehittymistä ja edistää niitä käyttävien palveluiden yleistymistä. Samalla tulisi kuitenkin huolehtia kansalaisten yksityisyyden suojan turvaamisesta. Luottamus on keskeinen tekijä sähköisten tunnistamismenetelmien ja näitä menetelmiä käyttävien sovellusten ja palvelujen kehittämisen, käytön ja yleistymisen kannalta. Alan toimijat ja sähköisen tunnistamisen menetelmien yleistyminen tarvitsevat selkeän ja myös oikeusvarmuuden osalta vakaan toimintaympäristön.

Liikenne- ja viestintäministeriön viestintämarkkinaosaston verkkoliiketoimintayksikkö päätti lähteä selvittämään yleisesti sähköisen tunnistamisen ja teknisen valvonnan sääntelyn ja muiden toimenpiteiden tarvetta erityisesti yksityisyyden suojan näkökulmasta. Erityisenä mielenkiinnon kohteena oli biometrisiin tunnisteisiin eli henkilön fyysisiin ominaisuuksiin perustuva tunnistaminen. Jo taustaselvitystä käynnistäessä oli selvää, että selvityksessä mahdollisesti ehdotettavat toimenpiteet eivät tule kuulumaan kaikilta osin ensisijaisesti liikenne- ja viestintäministeriön toimialaan. Tästä riippumatta selvityksen tehtävänasettelu haluttiin kokonaiskuvan muodostamiseksi pitää varsin laajana.

Tutkimuksessa selvitettiin erilaisten sähköisen tunnistamisen menetelmien ominaisuuksia, heikkouksia, vahvuuksia, sovelluskohteita ja tietoturvavaatimuksia sekä pyrittiin tältä pohjalta arvioimaan, edellyttävätkö nämä menetelmät erityisesti yksityisyyden suojan kannalta sääntelyä tai mahdollisia muita toimenpiteitä.

Taustaselvityksen teki konsulttityönä liikenne- ja viestintäministeriön toimeksiannosta Valimo Wireless Oy. Liikenne- ja viestintäministeriössä selvityksestä vastasi ylitarkastaja Juha Perttula.

Liikenne- ja viestintäministeriö haluaa kiittää niitä kaikkia lukuisia osapuolia, jotka joko asiantuntijoina tai muutoin edesauttoivat selvityksen valmistumista.

Helsingissä 14 päivänä lokakuuta 2003

Juha Perttula

SISÄLLYSLUETTELO

Kuvaluettelo

1 Yhteenveto

Tietoyhteiskunnan jatkuvan kehityksen myötä on nähtävissä ajankohtainen tarve rohkaista sähköisten tunnistusmenetelmien kehittymistä ja edistää niitä käyttävien palvelujen yleistymistä. Sähköisten tunnistusmenetelmien avulla yksilön identiteetti voidaan todentaa teknisin menetelmin, mikä luo mahdollisuuksia uusien sähköisten palveluiden ja teknisen valvonnan kehittymiselle.

Tunnistusmenetelmiä käyttävien asiointipalveluiden ja teknisen valvonnan yleistymistä tulee rohkaista, huolehtien kuitenkin samalla riittävästä yksityisyyden suojasta. Erityisesti uudet, lähinnä biometriset, tunnistusmenetelmät, jotka mahdollistavat yksilön automaattisen tunnistamisen siten, että tunnistettu ei välttämättä edes tiedä tulevansa tunnistetuksi, aiheuttavat riskin, joka liittyy yksilön oikeuteen pysyä anonyyminä. Tämä voi saada aikaan epätietoisuutta ja heikentää kansalaisten luottamusta käytettäviä teknisiä menetelmiä kohtaan. Yhteiskunnassa on turvattava yksityisyyden suojaan liittyen yksilön henkilökohtaisten tietojen suoja ja näitä tietoja koskevan itsemääräämisoikeuden toteutuminen.

1.2 Aihealue ja rakenne

Henkilön sähköinen tunnistaminen perustuu henkilöiden ominaisuuksiin, heidän hallussaan oleviin tietoihin tai muihin fyysisiin tunnisteisiin. Jotta henkilö pystytään tunnistamaan, tulee hänet yksilöivä ominaisuus olla sähköisesti luettavissa ja todennettavissa. Tämän raportin aluksi perehdytään henkilön sähköisen tunnistamisen periaatteisiin ja eri menetelmien vahvuuksiin ja heikkouksiin.

Eri tunnistusmenetelmien periaatteita, teknisiä ominaisuuksia sekä niiden vähimmäisvaatimuksia kuvataan muun muassa tietoturvan kannalta. Lisäksi eri teknologioita arvioidaan ja vertaillaan erityisesti luotettavuuden ja tunnistamisen varmuuden näkökulmasta. Teknisissä menetelmissä keskitytään kuvaamaan nykyisin yleisesti käytössä olevia menetelmiä, kuten käyttäjätunnuksilla ja salasanoilla sekä kertakäyttöisillä salasanoilla toteutettavaa tunnistamista. Lisäksi keskitytään yleistyviin ja kehittyviin menetelmiin, kuten varmennepohjaisiin ja biometrisiin tunnistusmenetelmiin.

Teknisten menetelmien arvioinnin ohella on pyritty hahmottamaa eri palvelu- ja sovellustilanteita, joissa tunnistamien on kriittisessä asemassa. Sekä teknisten menetelmien että palvelu- ja sovellusmallien kuvaamisessa keskitytään nykyisten menetelmien ja palveluiden lisäksi erityisesti niihin kehittymässä oleviin toimintamalleihin, jotka tulevat yleistymään lähitulevaisuudessa.

Teknisten menetelmien ja sovellus- ja palvelutilanteiden perusteella kuvataan niitä kriittisiä tilanteita, joissa yksityisyyden suoja saattaa vaarantua. Samalla keskitytään yksilön oikeuteen toimia anonyymisti sekä yksilön henkilötietoja koskevaan itsemääräämisoikeuteen.

Sääntelyn tai muiden toimenpiteiden tarvetta analysoidaan teknisten menetelmien ja mahdollisten palvelumallien pohjalta huomioiden yksilön suojan asettamat vaatimukset. Raportissa kuvataan niitä kriittisiä osa-alueita, jotka saatavat vaatia sääntelyä tai muita toimenpiteitä. Syy- ja seuraussuhteiden kuvaamisen ja arvioimisen kautta pyritään esittämään selkeitä ehdotuksia ja vaihtoehtoja mahdollisille toimenpiteille. Ehdotetut toimenpiteet ja erityisesti vaihtoehtoiset toimenpide-ehdotukset sisältävät hyvinkin pitkälle ulottuvia vaikutusketjuja, joiden positiivisia ja negatiivisia puolia on pyritty kuvaamaan. Näiden kuvausten perusteella voidaan tehdä lopulliset päätökset mahdollisista jatkotoimenpiteistä. Osa toimenpide-ehdotuksista sisältää suosituksen jatkotutkimuksesta tai –toimenpiteistä, päätöksenteon perustaksi.

1.3 Tutkimuksen työskentelymalli

Tämä tutkimus tehtiin Valimo Wireless Oy:n toteuttamana Liikenne- ja viestintäministeriön toimeksiannosta.

Tätä tutkimusta tehdessä tutustuttiin laajaan sekä kotimaiseen että kansainväliseen taustamateriaaliin teknisten menetelmien, kaupallisten palveluiden, yhteiskunnan ilmiöiden ja lainsäädännön osa-alueilta. Näistä ilmiöistä keskusteltiin lukuisten eri asiantuntijoiden kanssa.

Tärkeänä työskentelytapana käytettiin workshop-tyyppistä ryhmätyöskentelymallia, jonka avulla määriteltyjen osa-alueiden eri asiantuntijat osallistuivat työskentelyyn tarjoten arvokasta informaatiota ja näkemyksiä sekä kaupallisten toimijoiden että viranomaisten näkökulmista. Kaikki työskentelyyn osallistuneet henkilöt ilmaisivat mielipiteitä myös yksityishenkilöinä.

Raportissa on pyritty jäsentämään ja kuvaamaan työskentelyvaiheissa esille tulleita ilmiöitä, arvioimaan näiden pohjalta syy- ja seuraussuhteita ja tekemään toimenpide-ehdotuksia.

1.4 Yhteenveto tutkimustuloksista

Henkilön tunnistamisella tarkoitetaan henkilön identiteetin todentamista. Jotta henkilö voidaan sähköisesti tunnistaa, on henkilön yksilöivä ja henkilön hallussa oleva ominaisuus, piirre, tieto tai fyysinen tunniste oltava sähköisesti luettavissa ja todennettavissa.

Henkilön sähköinen tunnistaminen jakautuu kahteen eri käyttötilanteeseen: autentikointiin ja identifiointiin. Autentikoinnissa henkilö esittää väitteen omasta henkilöllisyydestään ja tämä väite tarkistetaan. Identifioinnissa henkilö pyritään tunnistamaan ilman henkilön esittämää väitettä hänen henkilöllisyydestään. Tyypillisesti autentikointia käytetään asiointipalveluissa ja identifiointia teknisessä valvonnassa sekä rikostutkinnassa.

Tunnistaminen voidaan jakaa myös passiiviseen tai aktiiviseen tunnistamiseen. Aktiivisessa tunnistamisessa tunnistettavalta henkilöltä vaaditaan aktiivista toimenpidettä. Passiivisessa tunnistamisessa tunnistamistilanne sen sijaan ei vaadi henkilöltä mitään toimenpiteitä. Passiivinen tunnistaminen on mahdollista ilman, että tunnistettava henkilö tietää tai ymmärtää tulevansa tunnistetuksi, mikä asettaa vaatimuksia yksilön suojan turvaamiselle erityisesti anonymiteetin säilyttämisen kannalta.

Tunnistamismenetelmät ja -teknologiat kehittyvät jatkuvasti. Kiistämättä yleisin tällä hetkellä käytössä oleva sähköinen tunnistusmenetelmä on käyttäjätunnuksiin ja salasanoihin perustuva menetelmä, joka puutteellisen tietoturvan johdosta soveltuu pääasiassa vain palveluihin, joissa ei käsitellä arkaluontoisia ja henkilökohtaisia tietoja, ja jotka eivät synnytä merkittäviä yksilösidonnaisia vastuita tai velvollisuuksia. Menetelmä ei myöskään sovellu yleiskäyttöiseksi tunnistusmenetelmäksi, jota käyttäjät ja palveluntarjoajat voisivat käyttää useissa eri palveluissa.

Käyttäjätunnuksen ja salasanan rinnalle on kehitetty kertakäyttöisiin salasanoihin perustuvia menetelmiä. Niillä on pyritty parantamaan tietoturvaa siten, että kerran käytetyn salasanan paljastumisesta ei ole hyötyä kenellekään, koska jokaisella käyttökerralla tarvitaan aina uusi salasana. Tällaisen menetelmän tietoturva on riittävällä tasolla ja se on käytössä muun muassa useissa verkkopankkipalveluissa. Ongelmana on tunnistustilanteiden heikko kiistämättömyys, menetelmän vaikeakäyttöisyys sekä menetelmän ylläpitoon liittyvät kalliit ja monimutkaiset prosessit.

Varmennepohjaisilla tunnistusmenetelmillä saavutetaan vahva tietoturva. Lisäksi laatuvarmenteet mahdollistavat luotettavan ja kiistämättömän tunnistamisen ja oikeudellisesti pätevän allekirjoituksen toteuttamisen. Varmennepohjaiset menetelmät tulevat yleistymään lähitulevaisuudessa teknologisen kehityksen ja teknologiaan liittyvien tukiprosessien kehittymisen myötä.

Biometrisiin ominaisuuksiin perustuvat tunnistamismenetelmät ovat kehittymässä nopeasti. Uudet teknologiat tuovat mukanaan erittäin vahvan tietoturvan sekä varmuuden tunnistamistapahtumalle. Biometriset ominaisuudet asettavat vaatimuksia lainsäädännöllisille toimenpiteille seuraavin perustein:

1. Biometrisessa tunnistamisessa henkilöstä luettua tai mitattua biometrista ominaisuutta verrataan samasta ominaisuudesta aiemmin otettuun tallenteeseen. Nämä tallenteet sisältävät tietoa yksilöön liitettävästä henkilökohtaisesta ominaisuudesta tai piirteestä.
2. Tunnistamiseen soveltuva biometrinen ominaisuus on pysyvä ja muuttumaton osa yksilöä.
3. Osa biometrisista ominaisuuksista on etäluettavissa ja mitattavissa ilman henkilön aktiivista toimenpidettä, mistä johtuen henkilö voidaan identifioida hänen tietämättään.

Näiden perusteiden pohjalta on määriteltävä hyväksyttävät menetelmät tunnistamiseen soveltuvien biometristen tietojen tallentamiselle, estää tallenteiden ei-hyväksyttävä ko-

pioiminen ja levittäminen sekä turvata yksilön itsemääräämisoikeus henkilötietojensa osalta. Lisäksi on määriteltävä vähimmäisvaatimukset tietoturvalle, jotta oikeudettoman tunnistamisen mahdollisuus pysyy mahdollisimman pienenä. Näillä toimenpiteillä turvataan yksilöiden luottamus palveluntarjoajiin ja viranomaisiin sekä turvataan palveluiden kehittyminen tasavertaisin ja yhdenmukaisin pelisäännöin.

Viranomaisten on turvattava yksilön suoja, markkinoiden toimivuus, yhteiskunnan turvallisuus ja pyrittävä edistämään tietoyhteiskunnan kehittymistä myös viranomaispalveluiden tuottajana. Viranomaisten on jatkossa otettava käyttöönsä nyt kehittymässä olevat tunnistamismenetelmät sekä omissa asiointipalveluissaan että yhteiskunnan järjestyksen ja turvallisuuden valvonnassa. Tällöin viranomaisten tulee myös harkita kyseisten järjestelmien ominaisuuksien ja toiminnallisuuksien tarjoamista myöskin kaupallisten toimijoiden käyttöön, tietoyhteiskuntaa sekä Suomen kilpailukykyä edistävinä keinoina.

Teknologian ja yhteiskunnan jatkuvasti kehittyessä kaikkia lähitulevaisuuden ilmiöitä ei ole voitu tämän tutkimuksen puitteissa selvittää ja analysoida. Suuri osa tämän tutkimuksen lopputuloksista ja toimenpide-ehdotuksista vaatii tarkempia lisätutkimuksia lopullisen jatkotoimenpidepäätöksen perusteeksi. On suositeltavaa, että lainsäädännössä ryhdytään välittömiin toimenpiteisiin tässä tutkimuksessa ilmenneiden uhkakuvien ja riskien minimoimiseksi ja mahdollisuuksien hyödyntämiseksi. Mahdollisimman aikaisella sääntelyllä ja lainsäädännön riittävällä uudistamisella pystytään säilyttämään luottamus tietoyhteiskunnan palveluihin parantaen yhteiskunnan toimivuutta, tehokkuutta sekä kansainvälistä ja kansallista kilpailukykyä.

1.5 Tiivistelmä ehdotetuista toimenpiteistä

Seuraavassa taulukossa on kuvattu lyhyesti tämän tutkimustyön tuloksena syntyneet toimenpide-ehdotukset. Taulukon toimenpide-ehdotukset on kuvattu yksityiskohtaisesti kappaleessa 7 ”Sääntelyn tarve”, jonka tekstiosuudessa viitataan myös taulukon numerointiin. Taulukon toimenpide-ehdotukset 6 ja 7 ovat vaihtoehtoisia tai toteutettavissa rinnakkaisina. Monet toimenpide-ehdotuksista ovat ehdollisia siten, että ne vaativat vielä lisäselvitysten toteuttamista.

Toimenpide-ehdotus		Toteutustapa	Tärkeysaste	Kiireellisyys
1.	Oikeudettoman biometrisen tunnistamisen säätäminen rangaistavaksi.	lainsäädännön muutos	välttämätön	välittömästi
2.	Nykyisen henkilötietolain soveltuvuuden tarkistaminen biometrian osalta.	lisäselvitys	välttämätön	välittömästi
3.	Biometrisen ominaisuuden tallentaminen sallittua ainoastaan henkilön suostumuksella.	lainsäädännön muutos	välttämätön	välittömästi

Toimenpide-ehdotus		Toteutustapa	Tärkeysaste	Kiireellisyys
4.	Biometrisen ominaisuuden rekisteröintiä koskeva ilmoitusvelvollisuus.	lainsäädännön muutos	vaatii toimenpiteitä	1-2 vuotta
5.	Biometrisen ominaisuuden tallentamisen ja rekisteröinnin ohjauksen ja valvonnan lisääminen.	tiedottaminen, valvonnan lisääminen	vaatii toimenpiteitä	1-2 vuotta
6.	Biometrisen ominaisuuden tallentaminen *sellaisenaan* kielletty.	lainsäädännön muutos	välttämätön	1-2 vuotta
7.	Biometrisen ominaisuuden tallentaminen *sellaisenaan* sallittu rekisteröitävän henkilön suostumuksella.	lainsäädännön muutos	vaatii toimenpiteitä	1-2 vuotta
8.	Ainoastaan hajautetut ja tunnistettavien henkilöiden hallussa olevat vertailurekisterit sallittu.	lainsäädännön muutos. Vaatii lisäselvitystä.	suositeltava	3-5 vuotta
9.	Vaatimus biometrisen rekisterin salaamiseksi siten, että vain rekisterinpitäjä voi käyttää tietoja.	lainsäädännön muutos. Vaatii lisäselvitystä.	suositeltava	3-5 vuotta
10.	Tunnistustilanteen kiistämättömyyden turvaaminen.	tiedottaminen, suositukset	suositeltava	3-5 vuotta
11.	”Laatubiotunnisteen” kehittäminen.	lainsäädännön muutos, järjestelmän suunnittelu ja toteutus. Vaatii lisäselvitystä.	suositeltava	3-5 vuotta
12.	Biometristen tunnisteiden käyttäminen viranomaisten tarjoamissa asiointipalveluissa.	vaatii laajan lisäselvityksen. (Oletettavasti vaatii muutoksia lainsäädäntöön.)	suositeltava	3-5 vuotta

2 Henkilön tunnistaminen

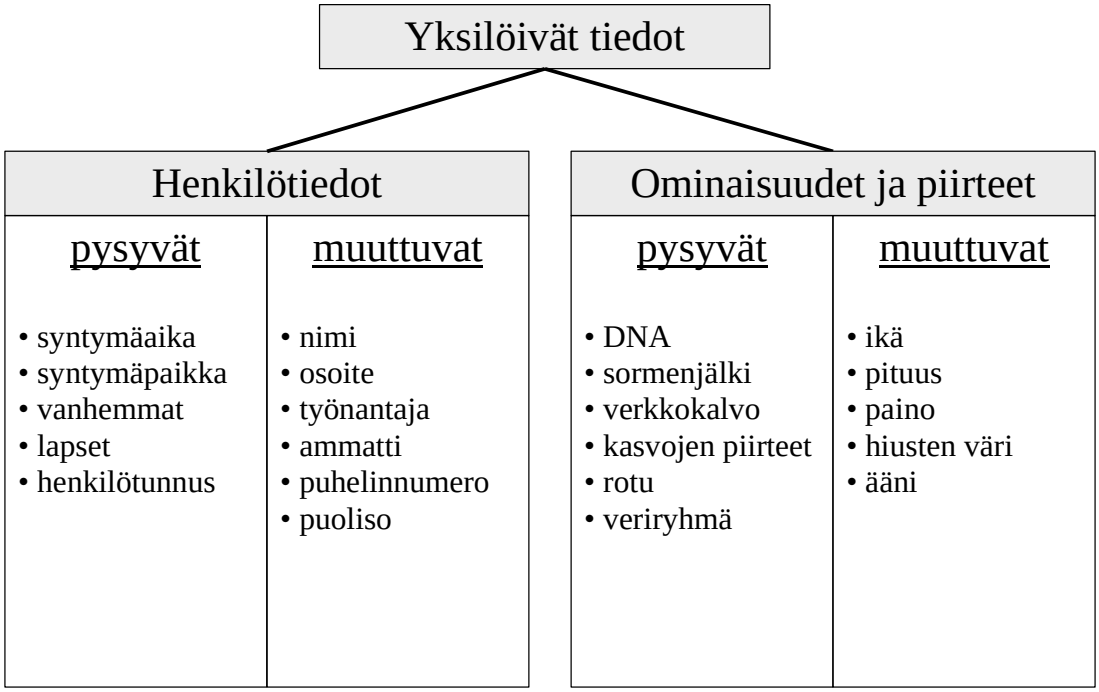
Kun fyysinen henkilö, yksilö, tunnistetaan, halutaan saada riittävällä varmuudella tieto kyseisen yksilön henkilöllisyydestä. Perinteisessä mielessä tällöin tunnistava taho vertaa yksilöstä tunnistamistilanteessa saatavissa olevia tietoja joihinkin varmoina pitämiinsä tietoihin, kuten aiemmin keräämiinsä tietoihin tai esimerkiksi henkilön esittämän henkilökortin tietoihin.

Yksinkertaisimmillaan tunnistaminen tapahtuu hyvinkin nopeasti ja automaattisesti esimerkiksi työtovereiden tavatessa toisensa joka päivä. Tällöin tunnistus tapahtuu tunnistajan havainnoidessa tunnistettavan ulkoisia piirteitä, kuten ulkoasua, puheääntä ja jopa eleitä tai käyttäytymistä. Yleensä toistensa kanssa usein asioivien henkilöiden kesken tunnistamien on niin nopea ja automaattinen prosessi, että osapuolet eivät edes huomaa sitä.

Monimutkaisimmillaan tunnistaminen voi olla useiden eri ominaisuuksien kartoittamista, etsimistä ja ristiinvertaamista eri rekisterien tietojen kesken. Tällöin tunnistettava henkilö ei usein joko kykene tai halua ilmaista tunnistamista helpottavia tietoja. Tämä on tyypillistä esimerkiksi rikostutkinnassa.

2.1 Yksilöivät tiedot ja ominaisuudet

Yksilön tunnistamisessa tunnistamistilanteessa saatuja tai havaittuja tietoja verrataan jo tiedossa oleviin tietoihin. Näiden tietojen tulee riittävällä varmuudella yksilöidä tunnistettava henkilö. Yksilöivät tiedot koostuvat yksilöön liittyvistä yksiselitteisistä henkilötiedoista ja yksilön ominaisuuksista. Nämä tiedot voidaan lisäksi jakaa pysyviin ja muuttuviin tietoihin.



Kuva 1: Henkilön yksilöivät tiedot ja ominaisuudet

2.1.1 Henkilötiedot

Yksilön identifioivia pysyviä henkilötietoja ovat syntymäaika ja -paikka sekä tiedot vanhemmista. Yhdessä nämä tiedot identifioivat yksilön henkilöllisyyden yksiselitteisesti: ei ole olemassa kahta henkilöä, joilla olisi samat vanhemmat ja joiden syntymäajat ja -paikat olisivat samat. Identtiset kaksoset ovat lähimpänä tätä määritelmää. Itse asiassa vanhempienkin tiedoista vain tieto äidistä on välttämätön.

Tiedot lapsista voidaan katsoa pysyviksi henkilötiedoiksi sillä luonnollisella lisäyksellä, että tieto lapsesta lisätään vasta lapsen syntyessä, ja sen jälkeen se on pysyvä henkilötieto.

Henkilötunnus voidaan katsoa pysyväksi ja yksilöiväksi tiedoksi, jos sen myöntävä viranomainen on sen sellaiseksi määritellyt. Huomioitavaa on, että henkilötunnus on keinotekoinen, ja se ei sellaisenaan yksilöi henkilöä, vaan se tarvitsee aina rinnalleen tiedot henkilötunnuksen määrittelijästä, eli yleensä tunnuksen myöntävästä viranomaisesta.

Muuttuvia henkilötietoja ovat yksilön nimi, osoite, puhelinnumero, tiedot työnantajasta jne. Muuttuvat henkilötiedot eivät koskaan yksiselitteisesti yksilöi henkilöä, mutta useampi näistä tiedoista yhdessä voi antaa riittävän varmuuden yksilön henkilöllisyydestä. Jos esimerkiksi tiedetään henkilön nimi ja osoite tiettynä ajankohtana, voidaan monissa käyttötilanteissa olla riittävän varmoja yksilön henkilöllisyydestä.

2.1.2 Ominaisuudet ja piirteet

Henkilön pysyvistä ominaisuuksista yksilöivin ja turvallisin on DNA. Se on jokaisella henkilöllä erilainen (poikkeuksena identtiset kaksoset ja kloonit) ja se pysyy koko elämän ajan muuttumattomana.

Muita henkilön pysyviä ominaisuuksia ovat esimerkiksi sormenjälki, silmän verkkokalvon rakenne ja kasvojen piirteet. Nämä pysyvät periaatteessa samana koko elämän ajan, mutta niissä tapahtuu muutoksia ihmisen luonnollisen kasvamisen ja vanhenemisen myötä. Vaikka pysyvissä piirteissä tapahtuu vanhenemisen myötä muutoksia, on niistä pystytty löytämään sellaisia piirteitä, jotka pysyvät riittävän tarkkoina koko elämän ajan, jotta yksilön henkilöllisyys voidaan todentaa näistä piirteistä riittävällä varmuudella. [1]

Henkilön muuttuvia ominaisuuksia ja piirteitä ovat luonnollisesti mm. ikä, pituus ja paino sekä esimerkiksi hiusten pituus ja väri. Nämä ominaisuudet soveltuvat erittäin huonosti henkilöllisyyden todentamiseen.

Lisäksi muuttuvina ominaisuuksina voidaan pitää esimerkiksi luonteenpiirteitä, ajatuksia, tietoja, taitoja ja kokemuksia. Kyseiset ominaisuudet ovat erittäin vaikeasti mitattavissa ja eivät sellaisenaan sovellu yksilön tunnistamiseen.

2.2 Yksilöivän tiedon mittaaminen ja taltiointi

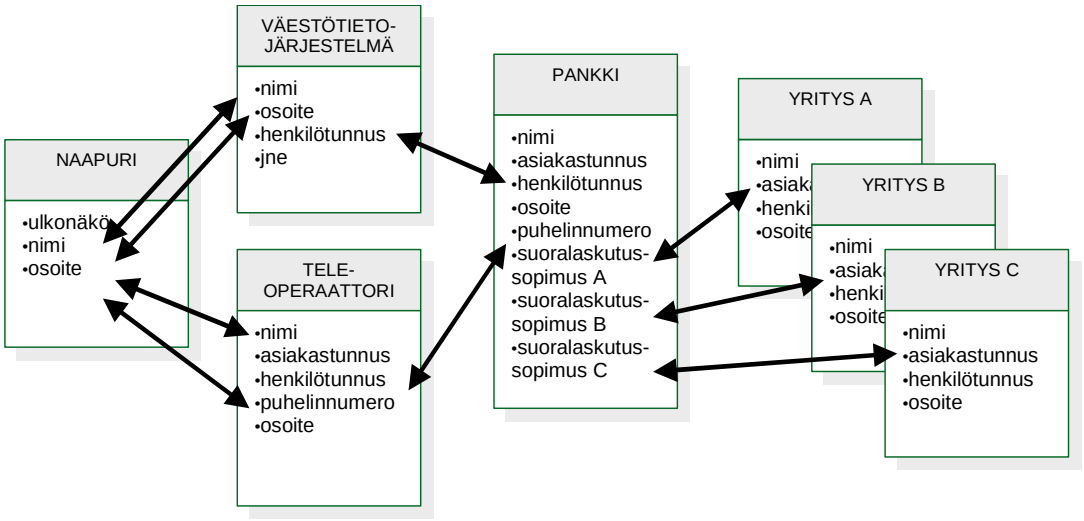
Henkilöstä on saatavilla sekä henkilötietoja että henkilön ominaisuuksia ja piirteitä, joiden voidaan nähdä kokonaisuutena muodostavan henkilön identiteetin.

Näistä henkilötiedoista ja henkilön ominaisuuksista ja piirteistä voidaan löytää tietoja, jotka joko yksin tai yhdessä yksilöivät kyseisen henkilön joko täysin yksiselitteisesti tai riittävällä varmuudella.

Vaikka jokin tieto yksinään pystyykin yksiselitteisesti yksilöimään henkilön, tiedosta ei kuitenkaan ole mitään hyötyä, ellei sitä pystytä erikseen yhdistämään tiettyyn henkilöön. Esimerkiksi henkilöstä ja hänen esittämästään sormenjäljestä tai DNA:sta ei ole hyötyä, ellei sille pystytä löytämään ”omistajaa” esimerkiksi sormenjälki- tai DNA-rekisteristä. Toisaalta vaikka rekisteristä löytyisikin tunnistettavan henkilön henkilötunnus, nimi- ja osoitetiedot, ei välttämättä ole varmaa, että rekisteriin on sitä luotaessa tallennettu oikeat tiedot.

Yksiselitteisestikin yksilöivän tiedon yhdistäminen tiettyyn henkilöön ja henkilön identiteettiin saattaa olla riippuvainen ketjusta tai verkosta erilaisia rekistereitä, ja kunkin tunnistustapahtuman luotettavuus voi siten riippua koko ketjun aukottomuudesta ja luotettavuudesta.

Esimerkkinä rekisteriketjusta ja -verkosta voidaan mainita tilanne, jossa asukas tunnistaa naapurinsa ulkonäön perusteella, ja tietää (ulkonäön lisäksi) kyseisen naapurin nimen ja osoitteen. Nimen ja osoitteen perusteella kyseiselle henkilölle voidaan löytää henkilötunnus väestötietojärjestelmästä. Henkilötunnuksen avulla henkilö voidaan löytää myös teleoperaattorin asiakastietokannasta ja saada selville hänen puhelinnumeronsa ja asiakastunnuksensa kyseisen operaattorin järjestelmässä. Vastaavasti puhelinnumeron perusteella hänet voidaan tunnistaa pankin puhelinpalvelua varten, jonka järjestelmästä taas voidaan löytää kyseisen henkilön henkilötunnuksen, osoitteen ja puhelinnumeron lisäksi esimerkiksi pankin asiakasnumero. Pankin suoralaskutussopimuksista kyseinen henkilö voidaan taas yhdistää eri yritysten asiakasrekistereihin, ja niin edelleen. Tällainen rekisteriverkko saattaa olla hyvinkin laaja ja se kasvaa aina, kun henkilö tekee uuden sopimuksen tai käyttää palvelua, johon hänen täytyy rekisteröityä.



Kuva 2: Henkilötietoja sisältävien rekistereiden muodostama verkko

2.2.1 Perinteisesti saatavat tiedot

Perinteisesti henkilötietoja on tallennettu kirjoittamalla. Esimerkiksi syntymäaika ja -paikka sekä vanhempien tiedot ja henkilön nimi ja osoite on kirjoitettu kirjaimin ja numeroin käyttäen tiettyjä nimeämisperiaatteita sekä kalenteri- ja aikastandardeja. Näiden tietojen mittaaminen ja tallentaminen on ajan myötä kypsynyt varsin suoraviivaiseksi prosessiksi, vaikka menetelmissä on eroavaisuuksia maailmanlaajuisesti tarkasteltuna. Hyvinä esimerkkeinä ovat muun muassa päivämäärän kirjoittamisen eri periaatteet Yhdysvaltojen ja Euroopan kesken sekä eri kalenteri- ja ajanlaskumenetelmät itäisen ja läntisen maailman kesken, puhumattakaan useista eri kirjoitusmerkeistä ja -menetelmistä.

Jokatapauksessa perinteisesti kirjoittamalla tallennetut tiedot on yleensä varsin suoraviivaisesti pystytty muuttamaan myös sähköiseen muotoon.

Perinteisiin menetelmiin voidaan laskea myös henkilön valokuvan tallentaminen ja sormenjälkien manuaalinen taltioiminen.

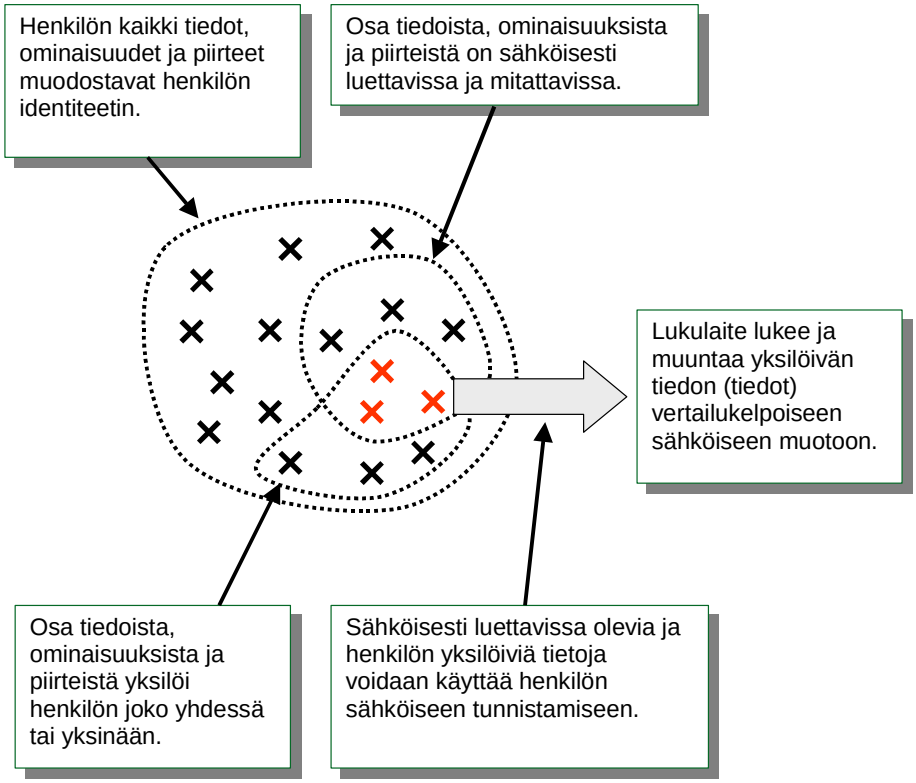
2.2.2 Sähköisesti luettavissa olevat tiedot

Lähes kaikki perinteisesti saatavissa olevat tiedot pystytään ”lukemaan ja mittaamaan” ja tallentamaan yksiselitteisesti myös sähköisessä muodossa. Viime vuosikymmeninä sähköisten menetelmien yleistyessä on löydetty keinoja, joilla myös henkilön sellaisia ominaisuuksia, joita ei perinteisin keinoin saada mitattua ja tallennettua, pystytään mittaamaan ja tallentamaan sähköisesti. Tällaisia uusia menetelmiä ovat muun muassa kasvojen piirteiden tallentaminen, silmän verkkokalvon rakenteen taltioiminen, DNA-rakenteen taltioiminen ja perinteisistä menetelmistä kehittyneet sormenjälkien rakenteiden taltioimismenetelmät.

Kun perinteisin menetelmin tallennetut tiedot ovat jokaisella käyttökerralla identtisiä (esimerkiksi syntymäaika on aina sama riippumatta milloin ja miten sitä kysytään) niin sähköisesti luettaville tiedoille on tyypillistä, että mittaustulos vaihtelee käyttökerrasta toiseen. Esimerkiksi sormenjäljen sähköinen lukeminen ja sähköisen mallin luominen tuottaa joka kerta hieman erilaisen lopputuloksen, riippuen muun muassa sormen asennosta ja puhtaudesta sekä mittalaitteen tarkkuudesta. Tästä syystä käytetyn luku-, mittaus- ja taltioimismenetelmän tulee olla sellainen, että eri lukukertojen tulosten eroista huolimatta menetelmä pystyy riittävällä tarkkuudella laskemaan mitattavasta piirteestä sellaisen sähköisen mallin, joka on aina luotettavasti yhdistettävissä alkuperäiseen mitattavaan piirteeseen tai ominaisuuteen.

Sähköisesti luettavien henkilötietojen ja henkilön ominaisuuksien ja piirteiden luotettava lukeminen, mittaaminen ja taltioiminen mahdollistaa kyseisten tietojen ja ominaisuuksien käyttämisen henkilön tunnistamiseen sähköisissä asiointipalveluissa ja teknisessä valvonnassa.

Seuraava kaaviokuva esittää henkilön tietojen, piirteiden ja ominaisuuksien sähköisen mittaamisen ja käyttämisen henkilön sähköiseen tunnistamiseen:



Kuva 3: Yksilön tietojen, ominaisuuksien ja piirteiden muodostama henkilön identiteetti

2.3 Käyttötilanteet ja roolit

Kun henkilö halutaan tunnistaa, käytettävä tunnistusmenetelmä ja sille asetettavat vaatimukset riippuvat käyttötilanteesta sekä ympäristöstä, jossa tunnistustilanne tapahtuu. Käyttötilanteeseen taas liittyvät asiointiosapuolet sekä heidän roolinsa kyseisessä tilanteessa.

Vaikka henkilö on eri tilanteissa aina sama fyysinen henkilö, vaikuttaa hänen roolinsa asiointilanteeseen ja siihen liittyviin oikeuksiin, vastuisiin ja velvollisuuksiin. Tilanne ei ole samanlainen, kun tietty henkilö asioi esimerkiksi pankissa yksityisenä henkilönä tai yrityksensä edustajana. Vaikka henkilö tunnistetaan juuri tietyksi yksilöksi, asiointitilanne ja henkilön rooli kyseisessä tilanteessa määräävät tilanteen mukanaan tuomat oikeudet, vastuut ja velvollisuudet.

Tyypillisessä asiointitilanteessa asiointikumppanien tunnistaminen perustuu menetelmään, jonka kaikki asiointiosapuolet hyväksyvät. Menetelmä voi perustua asiointiosapuolten kesken sovittuun ja kehitettyyn menetelmään, tai se voi olla jonkun ulkopuolisen osapuolen tarjoama menetelmä. Pääperiaatteena voidaan sanoa, että menetelmä ja sen luotettavuus on riittävä, jos asiointiosapuolet sen hyväksyvät. Jotta asiointiosapuolet voisivat jonkin tunnistamismenetelmän hyväksyä, tulee heidän kyetä joko itse arvioimaan käytetty menetelmä ja sen luotettavuus tai luottaa jonkun ulkopuolisen (esim. viranomaisen) antamaan vakuutukseen menetelmän luotettavuudesta.

3 Henkilön sähköinen tunnistaminen

Tunnistusmenetelmiä ja eri teknologioita käytetään yksilön henkilöllisyyden selvittämiseen tai varmentamiseen. Perinteisesti eri menetelmien toiminnallisuus ja luotettavuus perustuu seuraaviin oletuksiin:

1. Tunnistettavalla henkilöllä on esittää jokin tieto, jonka vain hän tietää.
2. Tunnistettavalla henkilöllä on esittää jokin fyysinen väline, jonka vain hän omistaa.
3. Tunnistettavalla henkilöllä on esittää jokin ominaisuus, joka on vain hänellä ja on osa häntä.

Edellä mainitut oletukset ovat hyvin yleisluontoisia, mutta sinänsä täysin toimivia ja paikkansapitäviä. Tunnistusmenetelmän luotettavuus kasvaa sitä mukaa mitä useamman edellä mainituista oletuksista menetelmä ottaa huomioon ja tarkistaa tunnistustilanteessa.

Ensimmäinen oletus perustuu siihen, että tunnistava taho ja tunnistettava henkilö ovat sopineet keskenään tietystä tiedosta, jonka vain he tietävät. Tieto on tyypillisesti henkilötunnus, asiakasnumero tai erikseen kyseistä tarkoitusta varten sovittu tai generoitu salasana. Ongelmana menetelmässä on sovitun tiedon leviäminen ja joutuminen vääriin käsiin.

Toinen oletus parantaa tilannetta sen verran, että tunnistettavan henkilön tulee pystyä esittämään jokin fyysinen väline, jonka hän omistaa. Tällöin edellisen kohdan sovittu tieto on yleensä talletettu kyseiselle välineelle. Menetelmä parantaa tilannetta vain, jos fyysisen välineen kopioiminen tai väärentäminen on riittävän vaikeaa. Tällöin voidaan olla riittävällä varmuudella varmoja siitä, että väline (ja sille tallennettu tunnistetieto) on vain yhden henkilön hallussa. Jos väline häviää tai varastetaan, sen oikean omistajan tulee havaita välineen katoaminen ja ilmoittaa siitä niille tahoille, jotka ovat hyväksyneet sen tunnistamisvälineeksi.

Kolmas oletus parantaa turvatasoa edelleen, koska tunnistettava henkilö ei voi kopioida tai luovuttaa ominaisuutta kenellekään, sillä se on osa häntä. Oletuksena tietysti on, että kyseinen ominaisuus on riittävän yksilöllinen ja helposti luettavissa ja tarkistettavissa. Jos henkilö voidaan täysin yksiselitteisesti ja luotettavasti tunnistaa ominaisuuden avulla, kahden ensimmäisen oletuksen soveltaminen ei tuo lisäarvoa tunnistamiselle. [3, 4, 5]

3.1 Autentikointi ja identifiointi

Henkilön tunnistamistilanteet jakautuvat kahteen eri alatyyppiin: autentikointiin ja identifiointiin.

3.1.1 Autentikointi

Autentikoinnilla tarkoitetaan tilannetta, jossa tunnistettava henkilö väittää olevansa tietty henkilö ja tämän väitteen oikeellisuus tarkistetaan. Rinnakkaisia termejä autentikoinnille ovat muun muassa tunnistaminen ja henkilöllisyyden varmentaminen ja englanniksi ”authentication” ja ”verification”. Autentikointiprosessin lopputuloksena saadaan tunnistettavan henkilön väitteelle joko vahvistus (”kyllä, henkilö on se, joka hän väittää olevansa”) tai hylkäys (”ei, henkilö ei ole se, joka hän väittää olevansa”). Autentikoinnin hylkäävän vastauksen mukana ei saada henkilön oikeaa identiteettiä, vaan henkilöltä on pyydettävä uusi väite henkilöllisyydestään. Usein käytännön sovelluksissa henkilöä ei päästetä jatkamaan palvelun käyttöä ennen kuin hänen autentikointinsa on onnistuneesti suoritettu.

3.1.2 Identifiointi

Identifioinnilla tarkoitetaan tilannetta, jossa tunnistettava henkilö ei esitä väitettä henkilöllisyydestä, vaan hänet tunnistetaan ilman mitään alkuoletuksia. Suomen kielessä identifioinnille rinnakkainen termi on niin ikään tunnistaminen. Englanniksi ilmiötä kuvaavia termejä ovat ”identification” ja ”recognition”.

Identifiointiprosessin lopputuloksena saadaan tunnistetun henkilön henkilötiedot (”Henkilö identifioitu Matti Möttöseksi, henkilötunnus 123456-0987”) tai tieto siitä, että henkilöä ei pystytty identifioimaan.

Käytännön sovelluksissa esiintyy kaksi erilaista identifiointitilannetta:

1. Henkilö pitää identifioida, ennen kuin hän pääsee jatkamaan esimerkiksi palvelun käyttöä. Tilanne on hyvin samantyyppinen kuin autentikoinnissa. Ainoa ero on, että henkilö ei esitä väitettä omasta henkilöllisyydestään.
2. Identifiointia käytetään tiettyjen henkilöiden, esimerkiksi etsintäkuulutettujen tai kadonneiden löytämiseksi. Jos henkilöä ei pystytä identifioimaan etsityksi henkilöksi, hän on vapaa jatkamaan. Olennaista tilanteessa on, että henkilö voi, järjestelmän niin salliessa, säilyttää anonymiteettinsä.

Vaikka identifioinnin ja autentikoinnin ero on periaatteellisella tasolla hyvin pieni, se on hyvä tiedostaa, sillä erityisesti teknisissä menetelmissä autentikointi- ja identifiointitilanteet ovat keskenään hyvinkin erilaiset, ja antavat toisistaan poikkeavat vaatimukset menetelmien toiminnallisuuden ja luotettavuuden kannalta. [1]

Teknisten eroavaisuuksien lisäksi autentikointi ja identifiointi eroavat toisistaan siinä mielessä, että autentikointitilanteessa käyttäjä menettää aina anonymiteettinsä, kun taas identifioinnissa se on mahdollista säilyttää, mikäli identifiointia käytetään esimerkiksi tiettyjen henkilöiden löytämiseksi.

3.2 Aktiivinen ja passiivinen tunnistaminen

Aktiivisessa tunnistamisessa henkilö ”ilmoittautuu” tunnistettavaksi. Henkilö esittää tunnistevälineensä, tai biometrisissä menetelmissä asettaa esimerkiksi sormensa lukulaitteeseen tai katsoo tietyn ajan tiettyyn pisteeseen tunnistamista varten. Tällöin tunnistettava henkilö on tietoinen tunnistustilanteesta ja saa yleensä myös tiedon tunnistamistapahtuman onnistumisesta ja tuloksesta.

Passiivisessa tunnistamisessa henkilö tunnistetaan ilman tunnistettavan aktiivista toimenpidettä. Tämä voi tapahtua esimerkiksi kadulla kuljettaessa valvontakameran kuvan perusteella. Toinen mahdollisuus on, että henkilöllä on esimerkiksi taskussaan etäluettava tunnisteväline (esim. RFID-teknologiaan perustuva toimikortti). Tällöin tunnistettava henkilö ei välttämättä tiedä tulleensa tunnistetuksi. Tämä ei kuitenkaan tarkoita sitä, että henkilö tunnistettaisiin ilman kyseisen henkilön suostumusta. Henkilö voi olla tietoinen siitä, että esimerkiksi tietyllä alueella kuljettaessa suoritetaan passiivista tunnistamista, ja hän voi olla antanut suostumuksensa tai hyväksyntänsä tälle toiminnalle.

On selkeästi nähtävissä, että tekniikan kehittyessä passiivisen ja aktiivisen tunnistamisen raja hämärtyy entisestään. Esimerkkinä voidaan todeta kuvitteellinen tilanne, jossa julkisen metro-verkoston käyttäjät identifioidaan ja heitä laskutetaan kasvotunnistuksen perusteella. Tunnistaminen vaatii katseen kohdistamista tiettyyn pisteeseen laiturialueen portille saavuttaessa, ja portti aukeaa kun identifiointi on onnistuneesti suoritettu. Tekniikan kehittyessä portit voidaan poistaa, ja tunnistaminen tapahtuu automaattisesti laiturialueelle sopivasti sijoitettujen kameroiden avulla. Esimerkissä aktiivinen tunnistaminen on muuttunut passiiviseksi, ellei aktiiviseksi tunnistamiseksi lueta laiturialueelle saapumista (olettaen, että sinne saapuva henkilö ymmärtää saapuvansa tilaan, jossa suoritetaan tunnistaminen).

Termit ”identifiointi” ja ”autentikointi” sekä ”aktiivinen” tunnistaminen ja ”passiivinen” tunnistaminen menevät jonkin verran päällekkäin. Autentikointi on käytännössä lähes aina aktiivista tunnistamista, sillä siinä henkilö tietoisesti ”saapuu” tunnistustilanteeseen ja väittää olevansa tietty henkilö. Identifiointi sen sijaan voi olla joko aktiivista tai passiivista tunnistamista, riippuen siitä, vaatiiko identifiointitilanne henkilöltä aktiivista toimenpidettä. Sen sijaan autentikointi, joka olisi passiivista tunnistamista on käytännössä erittäin harvinainen tilanne. Tällainen teoreettinen tilanne voisi olla mahdollinen, jos tunnistettavilla henkilöillä olisi aina esillä väite omasta henkilöllisyydestään (esimerkiksi kulkukortti tai vastaava) ja näitä väitteitä tarkistettaisiin jonkinlaisen lukulaitteen avulla siten, että tunnistaminen ei vaadi tunnistettavilta henkilöiltä erillisiä toimenpiteitä. [1]

Seuraavassa on esitetty yhteenvetona kaavio ja esimerkkejä autentikointi- ja identifiointitilanteista, joissa sovelletaan aktiivista ja passiivista tunnistamista:

	Aktiivinen	**Passiivinen**
Autentikointi ***authentication, verification***	Autentikointi on käytännössä aina aktiivista tunnistamista: Henkilö ”ilmoittautuu” tunnistettavaksi ja esittää väitteen omasta henkilöllisyydestään. Väite tarkistetaan. *Esimerkki: ”Olen Pekka Peloton, tässä tunnisteeni”.*	Käytännössä erittäin harvinainen tilanne: Tunnistettavien henkilöiden tulisi pitää esillä väitettä henkilöllisyydestään ja näitä väitteitä tarkistettaisiin ilman henkilöiden aktiivisia toimenpiteitä. *Esimerkki: Tietyssä tilassa olevilla henkilöillä on kuvallinen henkilökortti rintapielessä ja näitä henkilökortteja tarkistetaan valvontakameran avulla.*
Identifiointi ***identification, recognition, search***	Henkilö “ilmoittautuu” tunnistettavaksi, mutta ei esitä väitettä omasta henkilöllisyydestään. Henkilö tunnistetaan vertaamalla hänen biometrisia ominaisuuksiaan tietokannassa oleviin ominaisuuksiin. Jos henkilö tunnistetaan, tuloksena saadaan tieto henkilön henkilöllisyydestä. *Esimerkki: Henkilö saapuu rajatun alueen portille, jossa hän joutuu esittämään sormenjälkensä, jonka perusteella hänet yritetään tunnistaa.*	Henkilö tunnistetaan ulkoisten ominaisuuksiensa perusteella ilman, että hän ”ilmoittautuu” tunnistettavaksi ja että hän esittää mitään väitettä henkilöllisyydestään. *Esimerkki: Henkilö kävelee kadulla ja hänet tunnistetaan automaattisesti valvontakameran kuvasta.*

Kuva 4: Aktiivinen ja passiivinen autentikointi ja identifiointi

3.3 Suostumus tunnistustapahtumalle

Tunnistettavalle henkilölle on olennaista, että hänellä pysyy jonkinasteinen kontrolli tunnistustilanteisiin. Autentikoinnin ja identifioinnin sekä aktiivisen ja passiivisen tunnistamisen sijaan olisikin hyvä keskittyä siihen, onko tunnistettava henkilö tietoinen tunnistustilanteesta, ja onko hän antanut suostumuksensa passiivisesti tapahtuvaan tunnistamiseen.

Aktiivisessa tunnistamisessa ongelmaa ei esiinny, sillä tunnistustilanne vaatii aina tunnistettavan henkilön aktiivisen toimenpiteen. Kun henkilöltä pyydetään väitettä henkilöllisyydestä ja tunnistevälinettä, hän voi vielä halutessaan peruuttaa tunnistustapahtuman ja käyttää palvelua sellaisella vaihtoehtoisella tavalla, jossa henkilön anonymiteetti säilyy. Jos palveluntarjoaja ei tällaista vaihtoehtoa tarjoa, on henkilöllä vielä mahdollisuus olla käyttämättä kyseistä palvelua.

Sen sijaan passiivisessa tunnistamisessa ongelman aiheuttaa tunnistustilanteen automaattisuus. Henkilö tunnistetaan valvontakameran kuvan, äänitetyn puheen tai vastaavan havainnointilaitteen avulla automaattisesti ilman, että tunnistettava henkilö aktiivisesti ”ilmoittautuu” tunnistettavaksi. Tämä johtaa tilanteeseen, jossa henkilö voidaan tunnistaa automaattisesti ilman henkilön suostumusta.

Lisähaastetta tilanteelle aiheuttaa se, että passiivisessa tunnistamisessa suostumustietoja ei voida tallentaa mihinkään tietovarastoon, sillä henkilö pitäisi ensin tunnistaa, jotta tietovarastosta voitaisiin lukea, onko hän antanut suostumuksensa tunnistamiselle.

Yksi keino ratkaista ongelma on rajata selkeästi ne alueet, joilla passiivista tunnistamista tapahtuu ja informoida selkeästi alueelle saapuville henkilöille, että alueella suoritetaan automaattista tunnistamista. Tällöin, jos henkilö ei halua tulla tunnistetuksi, hän voi jättää menemättä kyseiselle rajatulle alueelle.

Toinen keino olisi kehittää menetelmä, jolla yksityiset henkilöt voisivat ilmaista luvan (tai kiellon) tunnistamiselle siten, että suostumus olisi automaattisesti luettavissa ennen tunnistustilannetta. Tällöin kaikkien täytyisi tietenkin luottaa tunnistajaan siinä mielessä, että tunnistaja ei tunnista niitä henkilöitä, jotka eivät ole antaneet suostumustaan.

3.4 Rekisteröinti

Jotta henkilö voidaan tunnistamistilanteessa tunnistaa, hänen antamiaan tai hänestä luettuja tunnistetietoja ja -ominaisuuksia verrataan aiemmin tietovarastoon tallennettuihin vertailutietoihin. Vertailutietojen lukemista ja tallentamista tietovarastoon kutsutaan rekisteröintiprosessiksi. Rekisteröintiprosessissa suoritetaan seuraavat alakohdat:

1. Henkilö ilmoittautuu rekisteröijälle rekisteröintiä varten.
2. Rekisteröijä varmentaa rekisteröitävän henkilön henkilöllisyyden jollakin luotettavalla ja hyväksyttävällä menetelmällä.
3. Rekisteröitävälle henkilölle määritellään tunnistetieto, joka teknologiasta riippuen voi olla esimerkiksi salasana, yksityinen avain tai sormenjälki.
4. Tunnistetiedosta lasketaan vertailutieto, joka yleensä on generoitu siten, että vertailutiedosta ei ole mahdollista laskea alkuperäistä tunnistetietoa.
5. Vertailutieto tallennetaan yhdessä henkilötietojen kanssa tietovarastoon.
6. Tunnistetieto jää henkilön haltuun.

Tunnistamistilanteessa vastaavasti henkilön antamista tai hänestä luetuista tunnistetiedoista lasketaan matemaattinen malli, jota verrattaan tietovarastoon talletettuihin vertailutietoihin. Tietovarasto voi olla keskitetty tai hajautettu käytetystä menetelmästä riippuen.

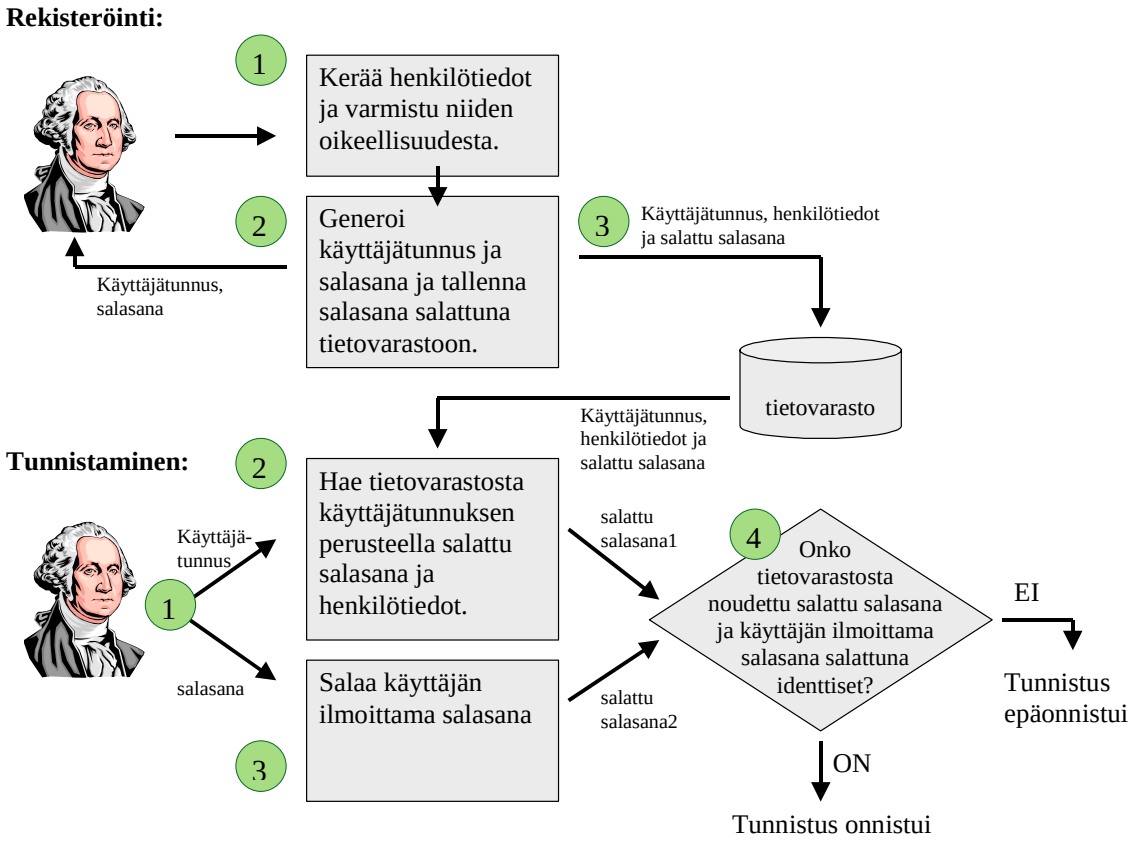
Rekisteröintiprosessin tulee olla erittäin luotettava. Jos rekisteröintiprosessissa tapahtuu virhe, kaikki prosessin jälkeiset kyseisellä menetelmällä ja tunnistetiedolla tehtävät tunnistustapahtumat antavat virheellisen tuloksen.

Rekisteröintiprosessit sekä tunnistustapahtumat vaihtelevat valitusta tunnistusmenetelmästä ja -teknologiasta riippuen. Tarkemmat kuvaukset löytyvät jäljempänä olevista kappaleista**.**

4 Tunnistusmenetelmät ja –teknologiat

4.1 Käyttäjätunnus ja salasana

Käyttäjätunnuksiin ja salasanoihin perustuva menetelmä on selkeästi yleisin sähköisissä palveluissa käytössä oleva tunnistusmenetelmä. Menetelmä perustuu siihen, että tunnistettava henkilö tietää itselleen kuuluvan käyttäjätunnuksen ja salasanan ja tunnistava taho tietää lisäksi käyttäjätunnukseen ja salasanaan liittyvät henkilötiedot. Seuraavassa kuvassa on kuvattu käyttäjätunnuksella ja salasanalla tehtävä rekisteröinti ja tunnistus.



Kuva 5: Käyttäjätunnukseen ja salasanaan perustuva rekisteröinti ja tunnistusprosessi

Rekisteröinti:

1. Tunnistettava henkilö saapuu rekisteröintipisteeseen, jossa rekisteröijä varmistaa henkilön henkilöllisyyden jollain hyväksyttävällä ja luotettavalla menetelmällä. Lisäksi henkilöstä kerätään tarvittavat henkilötiedot sekä mahdollisesti muuta tarpeellista lisätietoa.

2. Henkilölle luodaan käyttäjätunnus ja salasana, jotka luovutetaan rekisteröitävälle henkilölle.
3. Henkilön käyttäjätunnus, salasana salattuna ja henkilön henkilötiedot tallennetaan järjestelmän tietovarastoon.

Tunnistaminen:

1. Tunnistettava henkilö ilmoittaa käyttäjätunnuksensa ja salasanansa.
2. Tunnistava taho hakee järjestelmän tietovarastosta käyttäjätunnuksen perusteella kyseiselle käyttäjätunnukselle tallennetun salatun salasanan ja henkilötiedot.
3. Tunnistava taho salaa käyttäjän ilmoittaman salasanan, jota verrataan tietovarastoon tallennettuun salattuun salasanaan.
4. Jos tietovarastosta noudettu salattu salasana ja käyttäjän salasanasta laskettu salattu salasana ovat identtiset, tunnistus on onnistunut eli käyttäjä on antanut oikean käyttäjätunnuksen ja salasanan. Tällöin voidaan olettaa, että tietovarastoon tallennetut henkilötiedot kuuluvat käyttäjätunnuksen ja salasanan ilmoittaneelle henkilölle.

Menetelmän tietoturvaa voidaan pyrkiä parantamaa siten, että salasanat talletetaan salattuna tietovarastoon. Lisäksi salasanojen salausmenetelmä on sellainen, että salatusta salasanasta ei voida laskea alkuperäistä salasanaa. Tämän menetelmän tarkoituksena on parantaa tietovaraston turvallisuutta: Koska tietovarastoon tallennetut salasanat on salattu, niistä ei ole mitään hyötyä kenellekään ulkopuoliselle. Valitettavan usein salaus on jätetty toteuttamatta ja tietovarastoon on tallennettu salasanat sellaisenaan.

Käyttäjätunnuksen ja salasanan käyttäminen on sekä käyttäjälle että järjestelmän ylläpidolle varsin yksinkertaista ja helppokäyttöistä. Suurin ongelma on, että käyttäjätunnus ja salasana on helposti kopioitavissa. Loppukäyttäjät kirjoittavat käyttäjätunnuksia ja salasanoja usein paperille, jotta muistaisivat ne helpommin itse. Lisäksi käyttäjätunnuksia ja salasanoja luovutetaan toisille varsin huolettomasti, riippuen tietenkin kyseessä olevasta palvelusta.

Käyttäjätunnuksia ja salasanoja voidaan lisäksi saada selville arvaamalla sekä seuraamalla ja tallentamalla loppukäyttäjän näppäinten painalluksia tai tallentamalla verkkoliikennettä. Lisäksi epärehellinen palveluntarjoaja voi kokeilla tietyn henkilön rekisteröimää käyttäjätunnusta ja salasanaa muiden palveluntarjoajien palveluihin.

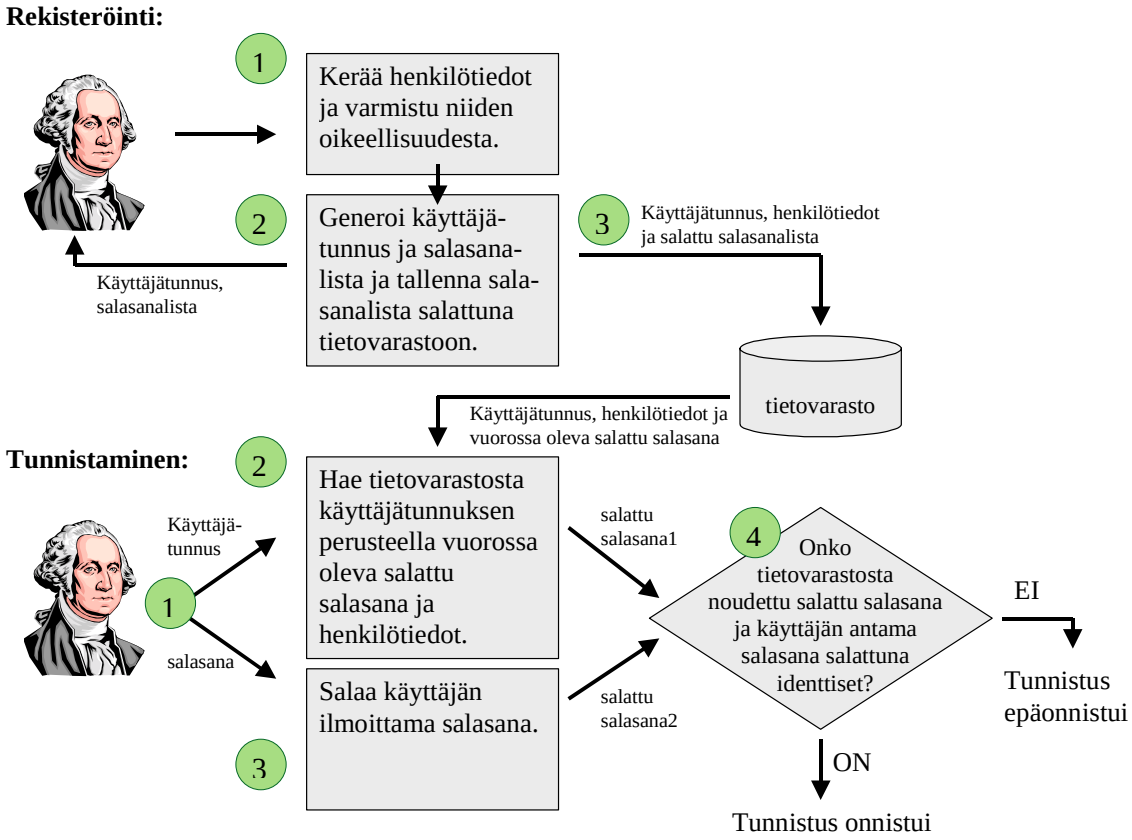
Lisäksi suuri ongelma on, että loppukäyttäjä ei välttämättä huomaa, jos hänen käyttäjätunnuksensa ja salasanansa ovat joutuneet vääriin käsiin. [3, 4, 5]

4.2 Kertakäyttösalasanat

Käyttäjätunnus, yhdistettynä kertakäyttöisiin ja vaihtuviin salasanoihin, poistaa salasanojen kopioimisesta, katoamisesta ja varastamisesta aiheutuvat ongelmat, sillä kukin

salasana on voimassa ainoastaan yhden käyttökerran. Jos joku ulkopuolinen saa selville käytetyn käyttäjätunnuksen ja salasanan, siitä ei ole hänelle mitään hyötyä. Menetelmä perustuu algoritmiin, jonka avulla voidaan generoida toisistaan riippumattomia satunnaisen näköisiä salasanoja. Tämä tarkoittaa, että kerran käytetystä salasanasta ei voida laskea seuraavana vuorossa olevaa salasanaa.

Rekisteröinti- ja tunnistusprosessit ovat hyvin samankaltaiset tavalliseen käyttäjätunnukseen ja salasanaan perustuvan menetelmän kanssa:



Kuva 6: Vaihtuvaan salasanaan perustuva rekisteröinti- ja tunnistusprosessi

Rekisteröinti:

1. Tunnistettava henkilö saapuu rekisteröintipisteeseen, jossa rekisteröijä varmistaa henkilön henkilöllisyyden jollain hyväksyttävällä ja luotettavalla menetelmällä. Lisäksi henkilöstä kerätään tarvittavat henkilötiedot sekä mahdollisesti muuta tarpeellista lisätietoa.
2. Henkilölle luodaan käyttäjätunnus ja salasanalista, jotka luovutetaan rekisteröitävälle henkilölle.
3. Henkilön käyttäjätunnus, salasanalista salattuna ja henkilön henkilötiedot tallennetaan järjestelmän tietovarastoon.

Tunnistaminen:

1. Tunnistettava henkilö ilmoittaa käyttäjätunnuksensa ja vuorossa olevan salasanansa.
2. Tunnistava taho hakee järjestelmän tietovarastosta käyttäjätunnuksen perusteella kyseiselle käyttäjätunnukselle tallennetusta salatusta salasanalistasta vuorossa olevan salasanan salattuna ja henkilötiedot.
3. Tunnistava taho salaa käyttäjän ilmoittaman salasanan, jota verrataan tietovarastoon noudettuun vuorossa olevaan salattuun salasanaan.
4. Jos tietovarastosta noudettu salattu salasana ja käyttäjän salasanasta laskettu salattu salasana ovat identtiset, tunnistus on onnistunut eli käyttäjä on antanut oikean käyttäjätunnuksen ja salasanan. Tällöin voidaan olettaa, että tietovarastoon tallennetut henkilötiedot kuuluvat käyttäjätunnuksen ja salasanan ilmoittaneelle henkilölle.

Käsite ”salasanalista” on hieman häilyvä ja se vaihtelee eri menetelmien kesken. Tyypillisesti salasanalistaan generoidaan tietty määrä salasanoja (esimerkiksi 100 kpl), jotka on käytettävä yksitellen oikeassa järjestyksessä. Käyttäjä yliviivaa käytetyn salasanan, jotta hän tietäisi mikä salasana on seuraavalla kerralla vuorossa tai käyttäjälle ilmoitetaan vuorossa olevan salasanan järjestysnumero. Kun kaikki salasanat on käytetty, käyttäjälle luodaan uusi lista, jota hän voi alkaa käyttää joko välittömästi tai kun vanha lista on käytetty loppuun. Menetelmä on Suomessa yleisesti käytössä pankkien internetpalveluissa.

Menetelmän huono puoli on, että salasanalista on yleensä tulostettuna paperille, joten se on edelleen kopioitavissa ja luovutettavissa eteenpäin. Käyttäjän kannalta huono puoli on, että salasanalistaa täytyy käytännössä aina pitää mukana, jotta se on käsillä kun käyttötarve ilmenee. Palveluntarjoajien kannalta huono puoli liittyy logistiikkaan: Kun käyttäjän salasanalista lähenee loppua, on käyttäjälle generoitava uusi lista, joka on tulostettava ja toimitettava käyttäjälle turvallisesti.

Edellä kuvattuja ongelmia on pyritty ratkaisemaan kehittämällä menetelmiä, joissa salasanalistaa ei generoida ennalta, vaan salasanojen generointi tapahtuu dynaamisesti käyttötilanteessa. Tällöin käyttäjälle annetaan jokin fyysinen laite, joka generoi ja näyttää aina uuden salasanan tietyn aikajakson, esimerkiksi minuutin, välein. Tällöin käyttäjä katsoo käyttötilanteessa laitteen näytöltä, mikä on kyseisellä hetkellä voimassa oleva salasana. Tämän menetelmän ansiosta ”salasanalista” ei ole kopioitavissa, sillä fyysisen laitteen, ja sen asetusten kopioiminen on käytännössä mahdotonta. Ongelmaksi muodostuu laitteen ja tunnistavan tahon järjestelmien pysyminen ajan suhteen synkronissa: Koska salasanan generoiminen (ja sen tarkistaminen) perustuu ajanhetkeen, on sekä salasanan generoijalla ja tarkastajalla oltava käytössään sama aika. Tämä aiheuttaa usein käyttötilanteissa ongelmia, jotka ratkaistaan synkronoimalla järjestelmät uudelleen. Sama ongelma ilmenee, jos laitteesta loppuvat patterit. Käyttäjän kannalta lisävaivaa aiheuttaa, että laitetta täytyy kantaa aina mukana käyttötilanteita varten. Tunnetuin tällainen menetelmä on RSA:n kehittämä SecurID-tuote.

Ehkäpä pisimmälle kehittynein kertakäyttöisiin salasanoihin perustuva menetelmä on järjestelmä, jossa salasana generoidaan aina kullakin käyttökerralla erikseen ja generoitu salasana lähetetään käyttäjän matkapuhelimeen tekstiviestipohjaisesti. Tunnistautuessaan järjestelmään käyttäjä syöttää käyttäjätunnuksensa, jonka jälkeen kertakäyttöinen ja satunnainen salasana generoidaan ja lähetetään käyttäjän matkapuhelimeen. Tämän jälkeen järjestelmä pyytää käyttäjää syöttämään kyseisen salasanan järjestelmään. Jos salasana on oikea, niin käyttäjä on tunnistettu. Tällöin salasanalistaa ei käytännössä ole olemassa, joten se ei myöskään ole kopioitavissa. Lisäksi järjestelmien ei tarvitse olla ajallisesti synkronissa, eikä järjestelmä vaadi erillistä tunnistuslaitetta, jota käyttäjän tulisi kantaa mukanaan (olettaen, että matkapuhelin on kuitenkin aina mukana). [3, 4, 5]

4.3 Varmennepohjaiset tunnistusmenetelmät

Varmennepohjaiset tunnistusmenetelmät perustuvat julkisen avaimen menetelmään (PKI = Public Key Infrastructure), jossa kullekin käyttäjälle generoidaan kahdesta avaimesta koostuva avainpari. Kun avainparin toisella avaimella salataan tietoa, niin salaus voidaan purkaa ainoastaan avainparin toisella avaimella. Avaimet luodaan siten, että niitä ei voida johtaa toisistaan.

Toinen avaimista nimetään julkiseksi avaimeksi ja toinen yksityiseksi avaimeksi. Menetelmä perustuu siihen, että julkinen avain on nimensä mukaisesti julkisesti kaikkien nähtävillä, ja yksityinen avain on ainoastaan omistajansa hallussa. Kun yksityisellä avaimella on salattu jotain tietoa, ja tiedon salaus puretaan onnistuneesti julkisella avaimella, voidaan olla varmoja, että alkuperäisen tiedon salanneella taholla on ollut hallussaan avainparin yksityinen avain. Menetelmää kutsutaan sähköiseksi allekirjoittamiseksi ja allekirjoituksen tarkastamiseksi.

Menetelmän luotettavuuden kannalta on ehdottoman tärkeää, että yksityinen avain on ja pysyy ainoastaan omistajansa hallussa. Tätä varten on luotu järjestelmiä, jossa yksityinen avain on suojattu siten, että sitä ei voida kopioida tai edes lukea; sillä voi ainoastaan tehdä toimenpiteitä.

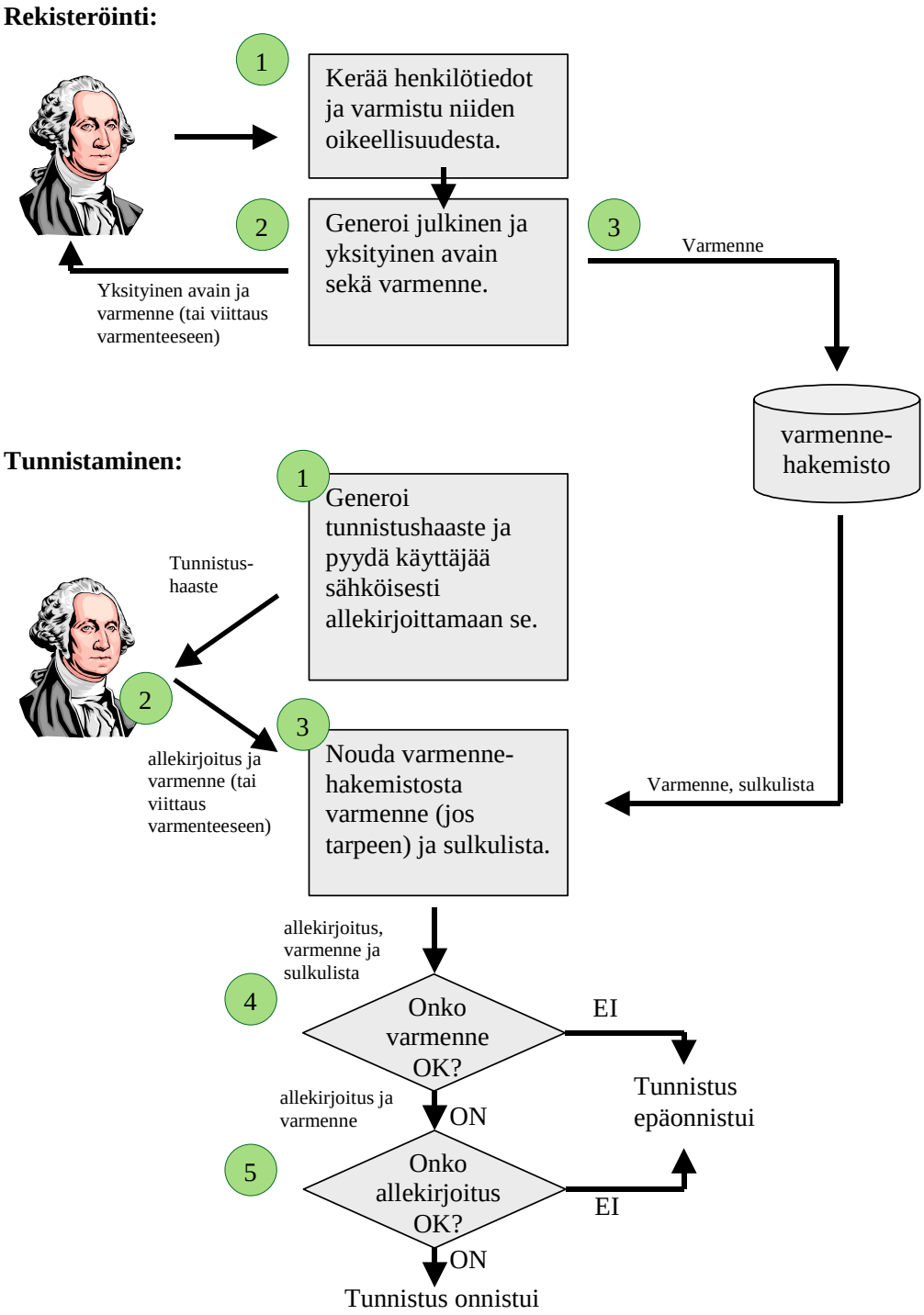
Toinen menetelmän luotettavuuden kannalta tärkeä seikka on sitoa avainpari luotettavasti omistajaansa. Tätä tarkoitusta varten kullekin käyttäjälle luodaan varmenne, joka sisältää käyttäjän julkisen avaimen ja käyttäjän henkilötiedot. Lisäksi varmenteen luova taho (varmenneviranomainen) allekirjoittaa sähköisesti luomansa varmenteen, jolloin voidaan varmistua siitä, että varmennetta ei ole varmenteen myöntämisen jälkeen muutettu.

Varmenteet julkaistaan varmennehakemistossa, josta käyttäjän varmenne ja sen sisältämät henkilötiedot ja julkinen avain voidaan tarvittaessa noutaa. Varmenne, tai vaihtoehtoisesti viittaus varmenteeseen, luovutetaan käyttäjälle.

Varmennehakemiston lisäksi julkaistaan sulkulista, joka sisältää tiedot niistä varmenteista, jotka on asetettu käyttökieltoon. Käyttökiellon syy on yleensä, että käyttäjän yksityinen avain on kadonnut tai päätynyt vääriin käsiin. Toinen mahdollinen syy on varmenteen tietojen paljastuminen virheellisiksi, varmenne on esimerkiksi kaikista turvatoimenpiteistä huolimatta myönnetty kuvitteelliselle tai väärälle henkilölle.

Kun varmenne on sulkulistalla, varmenteen julkista avainta vastaavalla yksityisellä avaimella tehtyjä toimenpiteitä ei voida hyväksyä, koska ei voida olla varmoja salaajan henkilöllisyydestä tai henkilöllisyyden oikeellisuudesta.

Seuraavassa on kuvattu varmenteisiin perustuvan tunnistusmenetelmän rekisteröinti- ja tunnistusprosessit.



Kuva 7: Varmenteisiin perustuva rekisteröinti- ja tunnistusprosessi

Rekisteröinti:

1. Henkilö saapuu rekisteröintipisteeseen, jossa rekisteröijä varmistaa henkilön henkilöllisyyden jollain hyväksyttävällä ja luotettavalla menetelmällä. Lisäksi henkilöstä kerätään tarvittavat henkilötiedot sekä mahdollisesti muuta tarpeellista lisätietoa.

2. Henkilölle generoidaan avainpari (julkinen ja yksityinen avain), joista yksityinen avain luovutetaan käyttäjälle. Julkinen avain ja henkilötiedot tallennetaan varmenteeseen. Varmenteen myöntäjä allekirjoittaa sähköisesti varmenteen. Käyttäjälle luovutetaan joko viittaus varmenteeseen tai itse varmenne.
3. Varmenne tallennetaan varmennehakemistoon.

Tunnistaminen:

1. Tunnistava taho generoi tunnistushaasteen, joka lähetetään tunnistettavalle henkilölle sähköisesti allekirjoitettavaksi. Tunnistushaaste voi olla periaatteessa mitä tahansa dataa; sen sisällöllä ei ole merkitystä. Tunnistushaasteen tulee olla kuitenkin jokaisella kerralla erilainen, jotta vältytään tietoturvariskiltä, joka syntyisi, mikäli joku kaappaisi allekirjoitetun haasteen ja pyrkisi käyttämään sitä uudelleen.
2. Käyttäjä allekirjoittaa tunnistushaasteen, eli salaa sen omalla yksityisellä avaimellaan. Allekirjoitus ja käyttäjän varmenne tai viittaus varmenteeseen lähetetään tunnistavalle taholle.
3. Tunnistava taho noutaa varmennehakemistosta käyttäjän ilmoittaman varmenneviittauksen perusteella käyttäjän varmenteen, jos käyttäjä ei ole sitä allekirjoituksen yhteydessä itse toimittanut. Varmennehakemistosta noudetaan lisäksi sulkulista.
4. Tunnistava taho tarkastaa varmenteen voimassaolon ja muuttumattomuuden. Voimassaolo tarkistetaan voimassaolopäiväyksestä sekä varmistamalla, että varmenne ei ole sulkulistalla. Varmenteen muuttumattomuus tarkastetaan tarkastamalla varmenteen myöntäjän varmenteeseen tekemä sähköinen allekirjoitus. Jos varmenteen voimassaoloaika on päättynyt, varmenne on sulkulistalla tai varmenteen myöntäjän tekemän sähköisen allekirjoituksen tarkastaminen epäonnistuu, käyttäjän tunnistaminen epäonnistuu.
5. Jos varmenne on hyväksyttävästi tarkastettu, tunnistava taho tarkastaa käyttäjän toimittaman tunnistehaasteen allekirjoituksen. Tällöin salattu tunnistushaaste (allekirjoitus) puretaan varmenteessa olevalla julkisella avaimella. Jos salauksen purun tuloksena saatu vastine on identtinen alkuperäisen tunnistushaasteen kanssa, tunnistus hyväksytään ja tunnistava taho voi olla varma, että tunnistushaasteen on allekirjoittanut henkilö, jolle varmenne on alun perin myönnetty. Jos allekirjoituksen tarkastaminen epäonnistuu, joku muu on allekirjoittanut tunnistushaasteen tai allekirjoitettu tunnistushaaste on muuttunut tiedonsiirron yhteydessä.

Menetelmän turvallisuuden kannalta ehkä kriittisin tekijä on yksityisen avaimen säilyminen omistajansa hallussa. Tätä varten on kehitetty sirukortteja, joissa avainpari generoidaan sirulla ja yksityinen avain jää turvaan sirulle, josta sitä ei voida lukea tai kopioida mitenkään. Sen sijaan avainparin julkinen avain on luettavissa sirukortilta. Tämän lisäksi sirukortilla on mahdollista tehdä toimenpiteitä, joissa käytetään sirulle tallennettua yksityistä avainta. Tällainen toimenpide on muun muassa juuri sähköinen allekirjoittaminen. Sirulla tehtävät toimenpiteet aktivoidaan yleensä tunnusluvulla, jonka ainoastaan käyttäjä tietää. Tällöin voidaan olla varmoja, että allekirjoittajalla on hallussaan

sirukortti ja sen käyttämiseen oikeuttava tunnusluku. Kuvatussa tilanteessa tunnistusmenetelmä toteuttaa kappaleen alussa kuvatuista oletuksista kaksi ensimmäistä.

Sirukortti voi olla pankkikortin kokoinen toimikortti (esimerkiksi HST-kortti), jolloin korttia käytetään esimerkiksi selainpohjaisissa palveluissa tietokoneella, johon on lisälaitteena hankittu kortinlukija ja siihen liittyvät ohjelmistot. Toisena yleistyvänä vaihtoehtona voidaan nähdä matkapuhelimen SIM-kortti, jolloin tunnistus- ja allekirjoituspyyntöjä voidaan lähettää käyttäjän matkapuhelimeen. [3, 4, 5]

4.4 Biometriset tunnistusmenetelmät

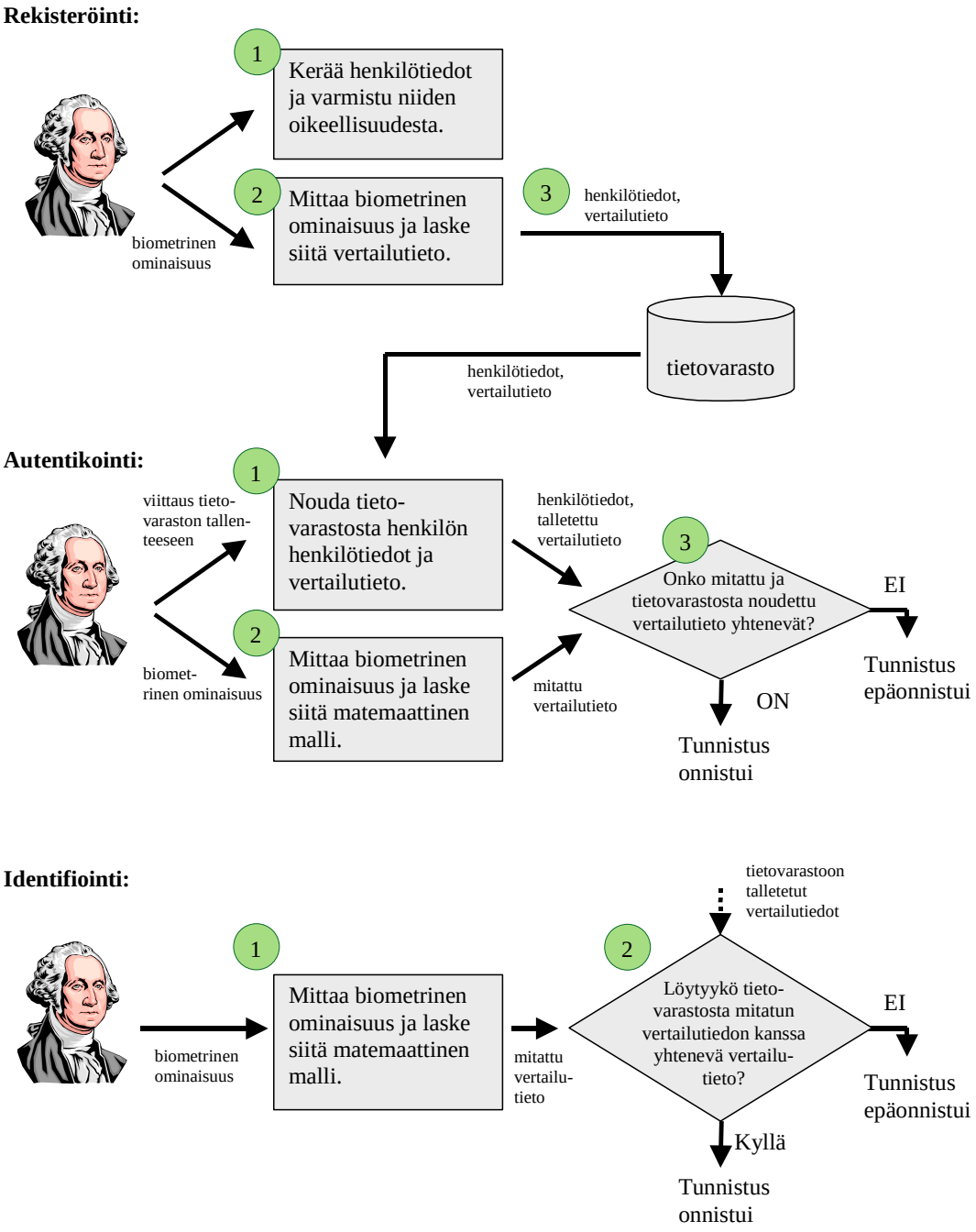
Biometrisissä tunnistusmenetelmissä henkilöstä mitataan jokin fyysinen ominaisuus, joka tallennetaan rekisteröintitilanteessa yhdessä henkilötietojen kanssa joko keskitettyyn tai hajautettuun tietovarastoon myöhempiä tunnistustilanteita varten. Tunnistustilanteessa ominaisuus mitataan uudestaan ja mittaustulosta verrataan tietovarastoon tallennettuun ominaisuuteen. Jos tunnistustilanteessa mitattu ominaisuus täsmää tietovaraston vertailuominaisuuden kanssa, henkilö on onnistuneesti tunnistettu. Tällöin henkilö on se, joka väittää olevansa.

Biometristä tunnistusmenetelmää voi käyttää edellä kuvatun autentikoinnin lisäksi identifiointiin, jossa henkilöstä luettua biometristä ominaisuutta verrataan kaikkiin tietovaraston vertailuominaisuuksiin. Jos tietovarastosta löydetään yhtenevä tallenne, on henkilö pystytty tunnistamaan ilman, että henkilö on esittänyt väitettä omasta henkilöllisyydestään (eli henkilö on identifioitu).

Jotta biometrinen ominaisuus soveltuisi henkilön tunnistamiseen, on ominaisuuden oltava riittävän yksilöllinen. Tällaiset ominaisuudet voivat perustua henkilön fyysisiin ominaisuuksiin tai henkilön käyttäytymiseen. Fyysisiin ominaisuuksiin perustuvia piirteitä ovat muun muassa sormenjälkien rakenteet, kämmenen muoto, kasvojen piirteet sekä silmän verkkokalvon ja iiriksen rakenteet. Käyttäytymiseen perustuvia identifioivia ominaisuuksia ovat muun muassa liikkumisen (kävelyn) liikeradat, käsialan piirteet ja puheäänen koostumus.

4.4.1 Rekisteröinti, autentikointi ja identifiointi

Seuraavassa on kuvattu biometrisen tunnistusmenetelmän rekisteröinti-, autentikointi- ja identifiointiprosessit.



Kuva 8: Biometriseen ominaisuuteen perustuva rekisteröinti-, autentikointi- ja identifiointiprosessi

Rekisteröinti:

1. Tunnistettava henkilö saapuu rekisteröitäväksi. Tunnistava taho varmentaa henkilön henkilöllisyyden jollakin hyväksyttävällä ja riittävän luotettavalla tavalla. Lisäksi henkilöstä kerätään tarvittavat henkilötiedot sekä mahdollisesti muuta tarpeellista lisätietoa.

2. Henkilöstä mitataan mittalaitteella biometrinen ominaisuus, josta lasketaan vertailutieto. Vertailutieto sisältää riittävän joukon mitattuja ominaisuuksia, joiden avulla tunnistaminen voidaan suorittaa luotettavasti tunnistustilanteessa.
3. Henkilön henkilötiedot sekä biometrisen ominaisuuden vertailutieto kootaan tallenteeseen, joka tallennetaan tietovarastoon. Tietovarasto voi olla keskitetty tai hajautettu. Hajautetussa mallissa tallenne luovutetaan tunnistettavalle henkilölle esimerkiksi tallennettuna toimikortille.

Autentikointi:

1. Autentikointitilanteessa tunnistettava henkilö esittää väitteen omasta henkilöllisyydestään. Tällöin hänen vertailutietonsa luetaan tallenteesta, jonka henkilö esittää (hajautettu tietovarasto), tai joka noudetaan tietovarastosta henkilön esittämän viitteen perusteella (keskitetty tietovarasto).
2. Tunnistettavasta henkilöstä mitataan mittalaitteella biometrinen ominaisuus, josta lasketaan matemaattinen malli, jota verrataan tietovaraston tallenteeseen tallennetun vertailutiedon kanssa.
3. Jos mitatusta ominaisuudesta laskettu matemaattinen malli ja tietovaraston tallenteeseen tallennettu vertailutieto ovat yhtenevät, on henkilö onnistuneesti autentikoitu. Tällöin henkilö on se, joka hän väittää olevansa ja hänen henkilötietonsa ovat luettavissa tietovaraston tallenteesta.

Identifiointi:

1. Henkilöstä mitataan biometrinen ominaisuus ja siitä lasketaan matemaattinen malli.
2. Mitatusta ominaisuudesta laskettua matemaattista mallia verrataan tietovarastoon tallennettujen vertailutietojen kanssa. Jos tietovarastosta löytyy tallenne, jossa on yhtenevä vertailutieto, on henkilö onnistuneesti identifioitu ja henkilön henkilötiedot ovat siten luettavissa kyseisestä tietovaraston tallenteesta.

Vaikka autentikointitapahtuma näyttäisi identifiointiin verrattuna olevan monimutkaisempi ja vaikeampi prosessi, itse asiassa identifiointi vaatii laitteilta enemmän resursseja ja kapasiteettia. Identifioinnissa mitattua ominaisuutta verrataan kaikkien tietovarastoon talletettujen vertailutietojen kanssa, kun taas autentikoinnissa mitattua ominaisuutta verrataan ainoastaan kyseisen henkilön vertailutietoon.

On huomattava, että identifiointi on mahdollista vain, jos järjestelmä on suunniteltu siten, että siinä käytetään keskitettyä tietovarastoa. Joissain tapauksissa yksityisyyden suojaa on pyritty turvaamaan hajautetun tietovaraston avulla, jolloin tunnistettavat henkilöt pitävät vertailutietoja mukanaan talletettuna esimerkiksi toimikortille. Tällöin tunnistaminen voi tapahtua vain tunnistettavan henkilön omasta tahdosta siten, että tunnistava taho mittaa biometrisen ominaisuuden ja vertaa sitä tunnistettavan henkilön hallussa olevalle toimikortille tallennettuun vertailutietoon. Turvallisuutta voidaan edelleen parantaa teknologisesti siten, ettei vertailutietoa edes voi lukea toimikortilta, vaan toimikortti suorittaa vertailun, ja ilmoittaa ainoastaan autentikoinnin tuloksen.

4.4.2 Epätarkkuudet ja todennäköisyydet

Biometrisessä tunnistamisessa on aina huomioitava, että fyysisen ominaisuuden mittaamisessa ja vertailutiedon generoinnissa tapahtuu aina epätarkkuuksia, lähinnä mitattavan ominaisuuden luonteesta ja mittalaitteen ominaisuuksista johtuen. Kun esimerkiksi sormenjäljet tai kasvojen piirteet kuvataan, ja kuvasta lasketaan vertailua varten tietomalli, voidaan olla varmoja, että sekä kuva että tietomalli ovat erilaiset jokaisella mittauskerralla. Tällöin eksaktia tietoa siitä, onko mitattu tietomalli yhtenevä vertailtavan tietomallin kanssa ei ole, vaan yhteneväisyys perustuu aina laskentamalliin, jonka tuloksena saadaan (yleensä) prosentuaalinen luku siitä, miten identtisiä vertailtavat tietomallit ovat.

Voidaankin ajatella, että biometrinen tunnistus perustuu aina todennäköisyyksiin: Autentikointitilanteessa järjestelmä kertoo kuinka varmasti tunnistettava henkilö on se, joka hän väittää olevansa, ja identifiointitilanteissa saadaan lista todennäköisyyksineen niistä henkilöistä, joita identifioitava henkilö eniten muistuttaa.

Kullekin mittaus- ja vertailumenetelmälle tulee asettaa rajat, milloin tunnistus on onnistunut ja milloin se on epäonnistunut.

4.4.3 Virhetilanteet

Edellä mainitut rajat riippuvat tunnistusmenetelmän ja -teknologian lisäksi käyttötilanteesta sekä vaadittavasta turvallisuustasosta. Mitä varmempia autentikointitilanteessa halutaan olla henkilön henkilöllisyydestä, sitä useammin täytyy varautua siihen, että syntyy tilanteita, joissa tunnistettavan henkilön mittaustulosta ja vertailua ei hyväksytä ja hän joutuu suorittamaan ominaisuuden mittaamisen ja vertailun uudelleen. Tällöin siis henkilö hylätään, vaikka hän on se, joka väittää olevansa. Virheellisesti epäonnistuneiden tunnistustapahtumien suhdetta onnistuneisiin tunnistustapahtumiin kutsutaan termillä *”false reject rate”* tai *”false nonmatch rate”*.

Vastaavasti, jos halutaan, että virheellisiä tunnistamisen epäonnistumisia tapahtuu mahdollisimman vähän, kasvatetaan riskiä siitä, että autentikointi antaa virheellisesti hyväksynnän vertailulle, jossa vertailun pitäisi antaa hylkäävä tulos. Tällöin siis henkilö hyväksytään, vaikka hän ei ole se, joka hän väittää olevansa. Tätä virheellisen hyväksynnän suhdetta oikein tapahtuviin hyväksymisiin kutsutaan termillä *”false acceptance rate”* tai *”false match rate”*.

Edellä mainitut virheet ovat autentikointitilanteiden lisäksi mahdollisia myös identifiointitilanteissa. Ensiksi kuvattu virhe tapahtuu, kun henkilöä ei identifioida, vaikka hänen vertailutietonsa on tallennettuna tietovarastossa. Jäljempänä kuvattu virhe tapahtuu, jos henkilö identifioidaan virheellisesti henkilöksi, joka hän ei ole.

Edellä mainittujen virheiden lisäksi biometrisissä menetelmissä on määriteltävissä kaksi virhetilannetta, joista ensimmäisessä mittalaite ei kykene saamaan biometrisesta omi-

naisuudesta riittävän laadukasta mittaustulosta. Tämä voi tapahtua esimerkiksi sormenjälkitunnistamisessa sormen likaisuudesta tai sormen virheellisestä asennosta johtuen. Kasvotunnistuksessa virhe voi johtua esimerkiksi riittämättömästä valosta tai liian kirkkaasta taustavalosta. Tätä virhetilannetta kutsutaan termillä *”failure to capture”* tai *”failure to acquire”*. Toinen virhetilanne voi syntyä rekisteröintitilanteessa, kun rekisteröitävältä henkilöltä ei saada riittävän laadukasta vertailuaineistoa. Tämä johtuu yleensä siitä, että rekisteröitävältä henkilöltä puuttuu tarvittava biometrinen ominaisuus (esimerkiksi sormenjälkitunnistuksessa puuttuu sormet). Tätä virhettä kutsutaan termillä *”failure to enrol”*. [1]

4.4.4 Ominaisuudet

Seuraavassa taulukossa on vertailtu eri biometristen menetelmien ominaisuuksia [1]:

	Sormenjälki	Kämmenen rakenne	Kasvotunnistus	Iris	Verkkokalvo	Sormen rakenne	Äänitunnistus	Allekirjoitus
täsmällisyys, tarkkuus	Hyvä	Hyvä	Hyvä	Erittäin hyvä	Erittäin hyvä	Keskiverto	Keskiverto	Keskiverto
helppokäyttöisyys	Hyvä	Hyvä	Melko hyvä	Melko huono	Huono	Hyvä	Hyvä	Hyvä
käyttäjien hyväksyntä	Melko huono	Melko hyvä	Hyvä	Melko hyvä	Huono	Melko hyvä	Hyvä	Melko hyvä
ominaisuuden muuttumattomuus, pysyvyys	Hyvä	Melko hyvä	Melko huono	Hyvä	Hyvä	Melko hyvä	Melko huono	Melko huono
erottuvaisuus, yksilöllisyys	Hyvä	Keskiverto	Huono	Erittäin hyvä	Erittäin hyvä	Keskiverto	Huono	Huono
mitattavuus, luettavuus	Keskiverto	Hyvä	Hyvä	Keskiverto	Keskiverto	Hyvä	Keskiverto	Keskiverto
suorituskyky	Hyvä	Keskiverto	Huono	Hyvä	Hyvä	Keskiverto	Huono	Huono
hyväksyttävyys	Keskiverto	Keskiverto	Hyvä	Huono	Huono	Keskiverto	Hyvä	Hyvä
väärinkäytön mahdollisuus	Matala	Keskiverto	Korkea	Matala	Matala	Keskiverto	Korkea	Korkea

	Sormenjälki	Kämmenen rakenne	Kasvotunnistus	Iris	Verkkokalvo	Sormen rakenne	Äänitunnistus	Allekirjoitus
Soveltuu autentikointiin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Soveltuu identifiointiin	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Ei	Ei	Ei
käytön este	jäljen kulunei suus, sormen tai käden menetys	käden menetys	kasvojen menetys	silmän tai näön menetys	silmän tai näön menetys	sormen tai käden menetys	äänen tai puhekyvyn menetys	käden tai motoriikan menetys

Kuva 9: Biometristen menetelmien ominaisuuksia

Edellä mainittujen menetelmien lisäksi kehitteillä on useita muita biometrisiä tunnistusmenetelmiä kuten esimerkiksi kävelytyyliin, puhetyyliin (suun liikkeisiin) sekä ominaishajuun perustuvia menetelmiä.

4.5 Teknologioiden luotettavuus ja tietoturva

Eri tunnistusmenetelmien luotettavuus ja turvallisuus vaihtelee erittäin paljon. Oikein käytettynä periaatteessa kaikki edellä kuvatut menetelmät ovat luotettavia, mutta turvallisuuden ja luotettavuuden takaamiseksi väärinkäyttö pyritään tekemään mahdollisimman vaikeaksi tai jopa mahdottomaksi.

4.5.1 Käyttäjätunnukset ja salasanat

Edellä kuvatuista tunnistusmenetelmistä käyttäjätunnuksiin ja salasanoihin perustuva menetelmä on kaikkein haavoittuvin. Järjestelmä on luotettava vain, jos salasanat pysyvät ainoastaan käyttäjien tiedossa. Tätä on kuitenkin vaikea toteuttaa, sillä käyttäjät kirjoittavat usein salasanoja muistilapuille tai käyttävät helposti arvattavissa olevia salasanoja. Muistamisen helpottamiseksi käyttäjät usein käyttävät useissa palveluissa samaa käyttäjätunnusta ja salasanaa, jolloin epärehellinen palveluntarjoaja voi yrittää käyttää oman palvelunsa käyttäjien tunnuksia ja salasanoja muihin palveluihin.

Tunnuksia ja salasanoja voidaan myös saada selville esimerkiksi seuraamalla verkkoliikennettä tai tallentamalla käyttäjän näppäinpainalluksia erityisen laitteen tai ohjelmiston avulla tai perinteisesti kameravalvonnalla. Tällöin on mahdollista, että epärehellinen taho tallentaa käyttäjätunnukset ja salasanat, ja käyttää myöhemmin niitä hyväkseen kirjautuessaan palveluihin tai järjestelmiin.

Menetelmä on periaatteessa aina murrettavissa kokeilemalla kaikkia mahdollisia salasanoja, mikä on nykyisten tietokoneiden laskentateholla ja verkkoliikenteen kapasiteetilla suhteellisen helppoa. Järjestelmät voidaan kuitenkin rakentaa myös siten, että järjestelmä havaitsee ja torjuu tällaiset niin kutsutut brute-force -hyökkäykset, esimerkiksi siten, että järjestelmä sulkee käyttäjätunnuksen, jos sille yritetään syöttää kolme kertaa virheellinen salasana.

Edellä kuvattujen teknisten keinojen lisäksi on hyvä tiedostaa, että epärehellinen taho voi esimerkiksi kiristämällä tai uhkaamalla saada selville käyttäjän tiedossa olevat käyttäjätunnukset ja salasanat.

4.5.2 Kertakäyttösalasanat

Tunnistusmenetelmä, joka käyttää vaihtuvia salasanoja on hieman edellä kuvattua järjestelmää turvallisempi. Siinä kerran käytetyn salasanan paljastuminen ei aiheuta tietoturvariskiä. Suurin riski liittyy ennalta generoituihin salasanalistoihin, jotka yleensä tulostetaan paperille tai luottokortin tyyppiselle ”turvakortille”. Tulostettu lista on kopioitavissa ja on siten mahdollista, että koko lista päätyy epärehellisen toimijan haltuun. Tämäkään ei ole tietoturvariski, ellei epärehellinen taho saa samalla käsiinsä käyttäjätunnusta, johon salasanalista liittyy ja tietoonsa palvelua, johon käyttäjätunnuksella ja salasanalla pääsee. Valitettavan usein käyttäjät kirjoittavat käyttäjätunnuksensa salasanalistaan, ja jo itse salasanalistan ulkoasusta voi päätellä mihin palveluun se antaa käyttöoikeuden.

Salasanalistan kopioimisen mahdollisuus poistuu, kun salasanat generoidaan dynaamisesti aina käyttötilanteessa. Tällöin salasanalistaa ei sellaisenaan ole olemassa, vaan käyttäjä katsoo vuorossa olevan salasanan fyysisestä laiteesta aina käyttötilanteessa. Tällöin riskinä on luonnollisesti laitteen joutuminen vääriin käsiin, jolloin erärehellisen tahon tulee niin ikään tietää myös palvelu ja käyttäjätunnus, johon laite liittyy, jotta itse laitteesta olisi hänelle hyötyä.

Toteutuessaan suurin kertakäyttöisiin salasanoihin liittyvä riski on salasanojen generointialgoritmin paljastuminen. Vaikka salasanat näyttävät ulkoisesti satunnaisilta, ne on generoitu jonkin algoritmin ja laskentamallin perusteella. Tämän laskentakaavan paljastuminen saattaisi mahdollistaa esimerkiksi koko salasanalistan salasanojen laskemisen, kun tiedossa on muutama peräkkäin käytetty salasana tai generoinnin perustana oleva ajanhetki.

4.5.3 Varmennepohjaiset menetelmät

Julkisen avaimen menetelmään sekä varmenteisiin perustuva tunnistamismenetelmä on erittäin luotettava. Järjestelmän perustana olevat laskentamallit ja algoritmit on kehitetty ja julkaistu vuosikymmeniä sitten, joten niiden turvallisuustasoa on voitu arvioida jo pitkään.

Teknisessä mielessä turvallisuuden kannalta tärkein seikka on yksityisen avaimen säilyminen vain käyttäjän hallussa. Tätä varten kehitetyt sirukorttiratkaisut nähdään hyvin turvallisina. Perusperiaatteena niissä on, että yksityistä avainta ei saada lainkaan sirukortilta ulos, vaan ainoastaan kortilla voidaan tehdä toimenpiteitä, joissa käytetään yksityistä avainta. Toimenpiteet on lisäksi yleensä turvattu PIN-koodilla, jolloin vain sirukortin omistaja voi aktivoida toimenpiteet. PIN-koodin säilyttämiseen liittyy tietenkin käyttäjätunnusta ja salasanaa vastaavat tietoturvariskit (liian helppo koodi, muistilaput, näppäilyjen tallentaminen, uhkailu, kiristäminen jne.).

Jonkinasteisena tietoturvariskinä voidaan lisäksi nähdä sirukorttien lukijalaitteet ja niiden ohjelmistot. Riski liittyy siihen, voidaanko olla varmoja esimerkiksi siitä, että lukijalaite tai -ohjelmisto ei tallenna käyttäjän PIN-koodeja, ja käytä niitä myöhemmin hyväkseen esimerkiksi tekemällä toimenpiteitä itsekseen ilman käyttäjän hyväksyntää.

Teknisen tietoturvan lisäksi varmennepohjaisissa menetelmissä luottamus varmenteen myöntäjään, eli varmenneviranomaiseen, on ensiarvoisen tärkeää. Koska varmenne liittää julkisen avaimen ja varmenteen omistajan (eli myös avaimen omistajan) tosiinsa, on ehdottaman tärkeää, että tuohon liitokseen voidaan luottaa. Luottamus varmenteen myöntäjään voidaan menettää, jos käy esimerkiksi ilmi, että varmentaja ei ole rekisteröintivaiheessa tarkistanut varmennettavien henkilöiden henkilöllisyyttä riittävällä tarkkuudella ja varmenteita on myönnetty väärille henkilöille. Lisäksi luottamus voi mennä, jos varmentaja generoi varmenteita kuvitteellisille henkilöille tai muuttaa varmenteiden tietoja ilman hyväksyttävää syytä. Varmentajan on myös pystyttävä pitämään ajantasaista ja täsmällistä sulkulistapalvelua, jotta luottamus voisi säilyä.

Varmentajien luotettavuuden arviointia varten on kehitetty laatuvarmentaja-menetelmä, jossa laatuvarmentaja-statuksen voi saada ainoastaan varmentaja, jonka prosessit ja tekniset menetelmät ja laitteet täyttävät tietyt kriteerit. Suomessa Viestintävirasto arvioi laatuvarmenteiden tarjoajia koskevien vaatimusten täyttymisen.

4.5.4 Biometriset menetelmät

Biometrisissä menetelmissä luotettavuuden ja tietoturvan merkitys kasvaa. Muissa menetelmissä tunnistamisen tulos on aina täsmällinen; henkilö joko on se, joka hän väittää olevansa tai sitten ei ole. Biometrisissä menetelmissä mukaan tulevat todennäköisyydet, jolloin tulokseksi saadaan, että henkilö on, tai ei ole, tietyllä todennäköisyydellä tai varmuudella tietty henkilö. Lisäksi menetelmän turvatason muuttaminen aiheuttaa aina ”sivuvaikutuksia”: Mitä varmempi tunnistaminen halutaan, sitä useammin täytyy varautua tilanteeseen, jossa henkilö joutuu antamaan biometrisen näytteensä useampaan ker-

taan, jotta hänet saadaan tunnistettua. Vastaavasti, mitä pienemmäksi edellä kuvatun kaltaisen tilanteen todennäköisyys halutaan, sitä useammin täytyy varautua tilanteisiin, joissa tunnistamisessa tapahtuu virhe, eli henkilö tunnistetaan väärin.

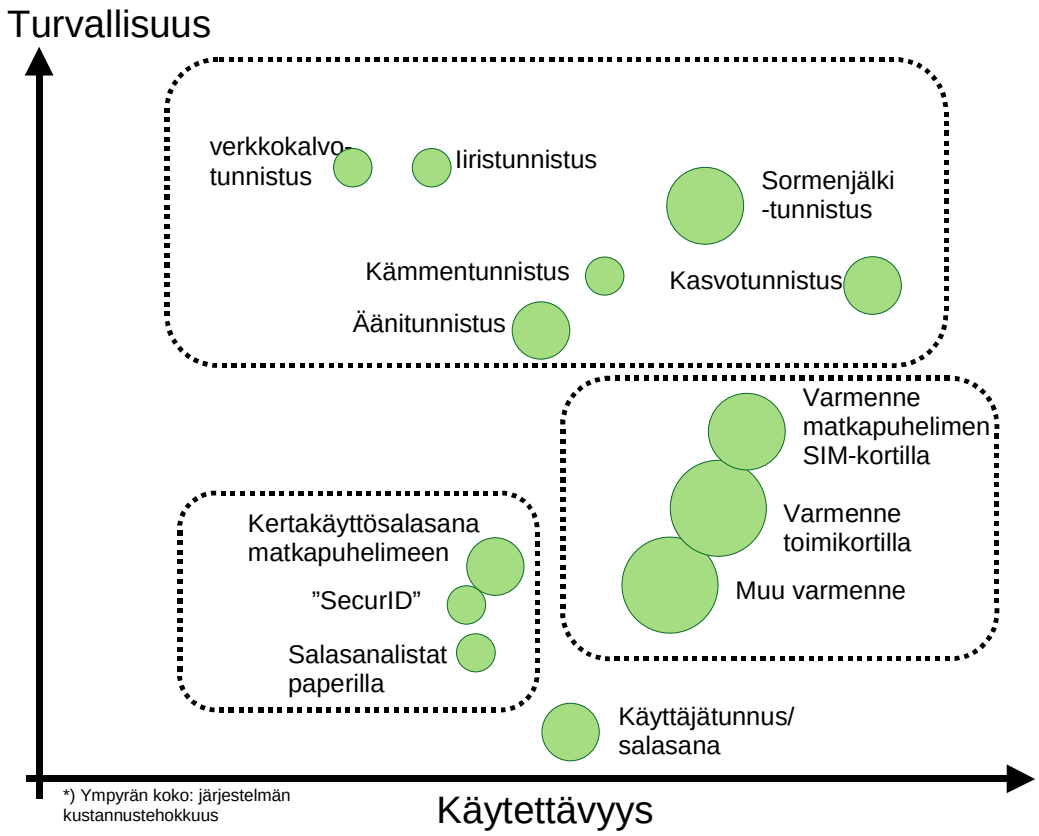
Seuraava esimerkki kuvaa hyvin tilannetta: Lentokentällä oleva rikollisia väkijoukosta etsivä biometrinen identifiointijärjestelmä on luonteeltaan sellainen, että yhdessä tapauksessa sadasta rikollista ei tunnisteta (vaikka hänet on järjestelmään tallennettu) ja väärintunnistamisen todennäköisyys on 0.001%. Tällöin järjestelmä havaitsee 99% varmuudella rikollisen, mutta tuottaa samalla suuren määrän vääriä hälytyksiä: Jos lentokentällä kulkee tarkastuspisteen läpi 200 000 henkilöä vuorokaudessa, vääriä hälytyksiä tapahtuu 200 kertaa päivässä. [1]

Biometrisissä menetelmissä luotettavuutta heikentää järjestelmien ja tunnistusalgoritmien monimutkaisuus. Järjestelmä antaa tuloksen, jonka verifiointi tai uudelleen laskenta on erittäin vaikeaa. Lisäksi tunnistettavien henkilöiden on vaikea varmistua oman vertailuaineistonsa oikeellisuudesta. Käyttäjätunnuksen ja salasanan oikeellisuudesta tai virheellisyydestä on helppo varmistua. PKI:hin perustuvien yksityisten ja julkisten avainten avulla tehdyt sähköiset allekirjoitukset on suhteellisen helppo manuaalisestikin tarkistaa, mutta biometrisen mallin oikeellisuus ja vertailukelpoisuus on vaikeasti auditoitavissa. Sekä tunnistettavien henkilöiden että järjestelmän käyttäjien on vain luotettava järjestelmään ja sen antamiin tuloksiin. Tämä luo selkeän tarpeen järjestelmien auditoinnille ja sertifioinnille.

Oman lisänsä tuo biometrisen ominaisuuden yksilöitävyys, pysyvyys, muuttumattomuus ja kopioimattomuus. Hyvä biometrinen järjestelmä ottaa lisäksi huomioon näytteen oikeellisuuden. Järjestelmä esimerkiksi tarkistaa, että sormenjälki tulee aidosta ja elävästä sormesta.

4.5.5 Teknologioiden vertailu

Seuraavaan kaavioon on koottu eri tunnistusteknologioita ja pyritty suuntaa-antavasti kuvaamaan teknologioiden turvallisuutta, luotettavuutta ja käytettävyyttä. Kuvassa menetelmän käytettävyys kasvaa siirryttäessä kaaviossa vasemmalta oikealle, ja menetelmän turvallisuus ja luotettavuus kasvaa alhaalta ylöspäin. Lisäksi ympyrän koolla on pyritty hahmottamaan järjestelmän kustannustehokkuutta järjestelmän ylläpitäjän kannalta: mitä suurempi ympyrä, sitä kustannustehokkaampi menetelmä. [1, 2, 3, 4, 5]



Kuva 10: Tunnistusteknologioiden vertailu

5 Palvelu- ja sovellusmahdollisuudet

Eri tunnistusmenetelmiä voidaan käyttää monentyyppisissä palveluissa ja sovelluksissa. Tyypillistä palveluille ja sovelluksille on, että tunnisteita ja tunnistusteknologioita käytetään vain teknisinä apuvälineinä. Kaikissa tilanteissa pääosassa on varsinainen asiointi- ja sopimussuhde ja sen mukana tulevat vastuut ja velvollisuudet, jotka halutaan tunnistamisen avulla sitoa luotettavasti asiointiosapuoliin.

5.1 Asiointipalvelut

Asiointipalveluilla tarkoitetaan tässä palveluja, joissa palvelun tarjoajana on kaupallinen yritys, kunnallinen tai valtiollinen organisaatio, viranomainen tai yksityinen henkilö ja palvelun käyttäjänä on vastaavasti yksityinen henkilö tai yrityksen tai organisaation edustaja. Sillä, onko palvelu sähköinen verkkopalvelu vai perinteinen kasvotusten tapahtuva palvelu, ei ole juurikaan merkitystä.

Palvelutilanteissa on tyypillistä, että käyttäjän tunnistamiselle on kaksi erillistä tarvetta: tunnistaminen käyttöoikeutta varten ja tunnistaminen tapahtuman hyväksymistä varten.

5.1.1 Tunnistaminen käyttöoikeutta varten

Käyttöoikeutta varten tapahtuva tunnistaminen tapahtuu siinä vaiheessa, kun käyttäjä ilmaisee halunsa ryhtyä käyttämään palvelua. Tällöin käyttäjä tunnistautuu ja hänelle annetaan pääsy palveluun. Tyypillistä näille palveluille on, että palvelua käyttäessään käyttäjällä on oikeus nähdä tietoa, joka on tarkoitettu vain kyseistä käyttäjää varten. Tiedot sisältävät yleensä käyttäjälle tärkeää henkilökohtaisia tai yksityistä tietoa. Palveluntarjoajan kannalta tunnistamisprosessin tarkoituksena on varmistua käyttäjän henkilöllisyydestä, jotta hänen nähtävilleen voidaan antaa oikeat tiedot. Toisaalta käyttäjän kannalta on tärkeää, että hän voi olla varma, että vain hänellä on pääsy häntä koskevaan aineistoon.

Tyypillisenä esimerkkinä tällaisesta palvelusta voidaan mainita pankkipalvelut (sekä perinteinen konttorissa tapahtuva palvelu että Internet-pankkipalvelu), joissa käyttäjä joutuu tunnistautumaan, ennen kuin hänelle voidaan luovuttaa esimerkiksi tilitietoja. Vastaavia esimerkkejä ovat osakevälityspalvelut, erilaiset viranomaispalvelut ja kaupalliset verkkokaupat.

Toinen tyypillinen käyttötilanne on yrityksen tai organisaation työntekijöilleen ja joissain tapauksissa asiakkailleen ja kumppaneilleen antama pääsy yrityksen tietojärjestelmään. Tällöin järjestelmässä on saatavilla tietoja, jotka eivät välttämättä ole kovin henkilökohtaisia, mutta tiedon omistaja haluaa rajoittaa tiedon jakelua ja leviämistä.

Sama analogia voidaan nähdä perinteisessä kulunvalvonnassa: henkilö joutuu tunnistautumaan päästäkseen esimerkiksi oman työpaikkansa tiloihin.

Edellä kuvatuissa esimerkeissä tunnistamiselle on nähtävissä selkeä tarve: pääsy rajoitettuun tietoon tai resurssiin. Hankalampi tilanne syntyy, kun palveluntarjoaja haluaa tunnistaa henkilöt oman toimintansa tehostamisen takia esimerkiksi tarjoamalla räätälöityjä palveluita tai hankkimalla asiakastietoja markkinointia varten. Tällöin esimerkiksi verkkokauppa haluaa tunnistaa asiakkaansa, jotta asiakkaalle voidaan esimerkiksi mainostaa tuotteita, joita samanikäiset ja samoista asioista kiinnostuneet henkilöt ovat verkkokaupassa tutkineet tai ostaneet. Vastaavasti tietoja saatetaan haluta kerätä myöhempää markkinointia varten, ja joissain tapauksissa palveluntarjoajan intressi kerätä asiakastietoja liittyy haluun myydä tietoja eteenpäin.

Edellä kuvatuista tilanteista seuraa kysymys siitä, milloin henkilön tunnistaminen on välttämätöntä. Esimerkiksi räätälöityä palvelua varten henkilön henkilöllisyyttä ei tarvita, riittää kun henkilöt pystytään yksilöimään ja erottamaan toisistaan. Niin ikään asiakasanalyysia varten asiakkaiden henkilöllisyydet ovat merkityksettömiä ja tarpeettomia: tärkeämpää on tietää asiakkaiden ominaisuudet, kuten ikä, sukupuoli, asuinpaikka jne.

Lisäksi voidaan pohtia tulisiko esimerkiksi verkkokaupan (tai vastaavan verkkopalvelun) asiakkaille taata mahdollisuus anonymiteettiin, sekä tuotteiden selailuvaiheessa että maksamisvaiheessa (kuten fyysisessä maailmassakin).

Tunnistaminen käyttöoikeutta varten tulee olla palvelun käyttäjän kannalta turvallista ja luotettavaa, sekä erityisesti helppokäyttöistä. Palvelun tarjoajan kannalta järjestelmän tulee olla niin ikään luotettava ja turvallinen, mutta myös kustannustehokas. Kustannustehokkuus ja osittain myös helppokäyttöisyys voidaan saavuttaa menetelmällä, joka on monikäyttöinen. Tällaisella menetelmällä voidaan tunnistautua useisiin eri palveluihin palveluntarjoajasta riippumatta. Turvallisuutta ja luotettavuutta voidaan parantaa järjestelmien auditoitavuudella ja sertifioinnilla. Järjestelmän tulee olla sellainen, että sekä palvelun käyttäjä että tarjoaja pystyvät luottamaan järjestelmään joko siten, että he itse ymmärtävät järjestelmän toiminnan tai luottavat ulkopuolisen tahon (esim. viranomaisen) antamaan hyväksyntään.

Perinteiset tunnistusmenetelmät, kuten käyttäjätunnus ja salasana, vaihtuvat salasanat ja varmennepohjaiset toimikortit ovat käytettävyydeltään varsin korkealla tasolla: käyttäjä syöttää käyttäjätunnuksen ja salasanan tai vastaavasti toimikortin ja PIN-koodin, ja hänet tunnistetaan. Aivan uuden käyttökokemuksen mahdollistavat biometriset menetelmät. Tällöin käyttäjä tunnistetaan jonkin fyysisen ominaisuuden perusteella. Esimerkiksi fyysinen pääsyn valvonta voidaan suorittaa siten, että ovi tai portti aukeaa syöttämällä sormi lukijalaitteeseen tai kääntämällä kasvot hetkeksi kameraa kohden. Riippuen palvelusta, fyysiseen pääsyn valvontaan voidaan liittää myös maksutapahtuma siten, että tiettyyn tilaan saapuminen aktivoi maksun. Esimerkkinä tällaisesta voidaan mainita julkinen liikenne, elokuvateatterit ja vastaavat palvelut, joissa maksua vastaan saadaan jokin kertaluonteinen palvelu.

5.1.2 Tapahtuman hyväksyminen

Tapahtuman hyväksymisellä tarkoitetaan palvelun tarjoajan ja käyttäjän tekemän tapahtuman, esimerkiksi sopimuksen, hyväksymistä. Tällöin osapuolet tekevät sopimuksen, jonka molemmat osapuolet hyväksyvät, ja ovat valmiita vastaanottamaan sopimuksen mukanaan tuomat vastuut ja velvollisuudet. Tällöin asiointiosapuolten tulee olla varmoja toistensa henkilöllisyyksistä ja heillä tulee olla käytössään jokin hyväksyttävä ja luotettava menetelmä sopimuksen kiistämättömyyden turvaamiseksi.

Teknisessä mielessä ainoa riittävän turvallinen ja kiistämätön menetelmä on varmennepohjainen sähköinen allekirjoitus. Menetelmän avulla asiointiosapuolet voivat todentaa allekirjoitetun sopimuksen sisällön ja allekirjoittajan henkilöllisyyden.

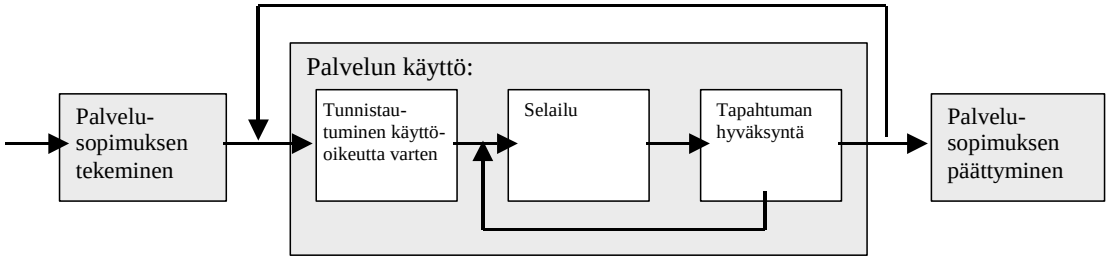
Varmennepohjaiseen sähköiseen allekirjoitukseen pätee samat tietoturvavaatimukset kuin varmennepohjaiseen tunnistamiseen (katso kappaleet 4.3 Varmennepohjaiset tunnistusmenetelmät ja 4.5.3 Varmennepohjaiset menetelmät).

Tällä hetkellä luotettavana ja hyväksyttävänä tekniikkana tapahtuman hyväksymiseen voidaan nähdä toimikorttipohjainen varmenteisiin perustuva sähköinen allekirjoitus. Siinä allekirjoitus luodaan toimikortin sirulla, jonka allekirjoitustoiminnallisuudet aktivoidaan PIN-koodilla. Käyttäjä tunnistautuu kortille ja antaa kortille luvan suorittaa sähköinen allekirjoittaminen. Menetelmän tunnistamisen (luvan antamista kortille) luotettavuutta voidaan parantaa biometrisellä tunnistamisella, esimerkiksi sallimalla allekirjoituksen aktivoinnin tapahtuvan vain sormenjäljen tai verkkokalvon tunnistamisen perusteella. Tällöin itse kortti varmistaa biometrialla käyttäjän henkilöllisyyden, ennen allekirjoituksen suorittamista.

Sähköisellä allekirjoituksella voidaan hyväksyä tapahtumia ja luoda sopimussuhteita. Tapahtuman hyväksyminen on tyypillistä silloin, kun palvelusta ostetaan tai tilataan jokin hyödyke, jolloin osto tai tilaus ja maksuehdot vahvistetaan sähköisellä allekirjoituksella. Sopimussuhde voidaan luoda esimerkiksi silloin, kun tilataan palvelu, jonka maksu määräytyy käyttötilanteiden tai -kertojen perusteella. Tällainen palvelu voi olla esimerkiksi joukkoliikenteen käyttäminen, josta veloitetaan kuljettujen matkojen perusteella. Tällöin henkilön tunnistaminen voi käyttötilanteessa tapahtua esimerkiksi biometrisen tunnistamisen perusteella.

5.1.3 Asiointipalvelun elinkaari

Asiointipalvelujen elinkaaren voidaan nähdä jakautuvan seuraaviin osa-alueisiin:



Kuva 11: Asiointipalvelun elinkaari

1. Palvelusopimuksen tekeminen: Palvelun tarjoaja ja käyttäjä sopivat palvelun käyttöehdoista sopien yksityiskohtaisesti sopimuksen voimassaolosta, maksuehdoista, toimintatavoista ja muista tarpeellisista palvelun käyttöön liittyvistä asioista.
2. Palvelun käyttö koostuu yhdestä tai useammasta käyttökerrasta riippuen palvelun luonteesta ja palvelusopimuksen ehdoista. Kukin käyttökerta koostuu seuraavista osa-alueista:
    a. Tunnistautuminen palveluun. Käyttäjä tunnistautuu palveluun palvelusopimuksessa määritellyllä tavalla.
    b. Selailuvaihe: Käyttäjä käyttää palvelua selaillen ja tutkien palvelun tietoja, ja tehden mahdollisesti alustavia päätöksiä jonkin tuotteen tai palvelun ostamisesta tai hankkimisesta.
    c. Tapahtuman hyväksyntä: Käyttäjä vahvistaa tuotteen tai palvelun ostamisen tai hankinnan hyväksyen samalla tilaus- tai hankintaehdot.
3. Palvelusopimuksen päättyminen. Käyttäjän käyttöoikeus kyseiseen palveluun päättyy.

Seuraavassa taulukossa on esitetty muutamia palveluesimerkkejä ja kuvattu olennaisimmat tilanteet, joissa käytetään sähköistä allekirjoitusta ja käyttäjän tunnistamista.

	Palvelusopimuksen tekeminen 	**Tunnistautuminen käyttöoikeutta varten:** 	**Selailu:**	**Tapahtuman hyväksyntä** 
Yrityksen tieto-järjestelmä:	Käyttäjä hyväksyy sähköisellä (tai perinteisellä) allekirjoituksella käyttösopimuksen.	Käyttäjä joutuu tunnistautumaan, jotta saa pääsyn rajoitettuun tietoon	Käyttäjä tutkii tietoja, dokumentteja, raportteja jne.	
Pankkipalvelu:	Käyttäjä hyväksyy sähköisellä (tai perinteisellä) allekirjoituksella palvelusopimuksen.	Käyttäjä joutuu tunnistautumaan, jotta saa näkymän omiin pankkitietoihinsa.	Käyttäjä tutkii tilitietojaan, velkoja, sijoituksiaan jne.	Käyttäjä hyväksyy tilisiirron sähköisellä allekirjoituksella
Verkkokauppa:			Anonyymi käyttäjä tutkii tuotteita ja kerää niitä ostoskoriin.	Käyttäjä hyväksyy tilauksen sähköisellä allekirjoituksella.
Joukkoliikenne / Elokuvateatteri	Käyttäjä hyväksyy sähköisellä (tai perinteisellä) allekirjoituksella sopimuksen, jossa sitoutuu maksamaan käytön perusteella palvelusta	Käyttäjä tunnistetaan ja veloitus koostuu käyttökertojen perusteella.	Käyttäjä käyttää palvelua	

Kuva 12: Palvelu- ja sovellusesimerkkejä

Kuten esimerkeistä käy ilmi, kaikki palvelut eivät vaadi palvelusopimusta tai edes tunnistautumista palvelun käyttöoikeutta varten. Tyypillinen esimerkki on verkkokauppa, jossa käyttäjä voi anonyymisti selailla ja valita tuotteita ostoskoriin, ja tunnistaminen suoritetaan vasta ostoskorin tuotteiden tilauksen ja maksun vahvistamisen yhteydessä.

Lisäksi nähdään, että kaikki palvelut eivät palvelun luonteesta johtuen sisällä tapahtumia ja sopimuksia, jotka vaatisivat tapahtuman luotettavaa ja vahvaa hyväksyntää.

Kun henkilö on tehnyt palveluntarjoajan kanssa palvelusopimuksen, ja sopinut siinä tunnistamismenetelmistä ja tunnistamistilanteiden mukana tuomista vastuista ja velvollisuuksista, uudet tunnistusteknologiat eivät periaatteessa muuta tilannetta mitenkään. Uusi teknologia ainoastaan helpottaa palvelun käyttöä ja tehostaa palveluprosesseja sekä käytössä olevien menetelmien luotettavuutta ja turvallisuutta. Joissakin tilanteissa saattaa olla, että palveluntarjoaja uskaltaa käynnistää palvelun vasta, kun riittävän turvallinen tunnistusteknologia on käytettävissä, vaikka käyttäjä olisikin jo valmis tekemään sopimukseen.

5.2 Valvonta

Asiointipalvelujen käyttötilanteista generoituvaa käyttötietoa on mahdollista käyttää tekniseen valvontaan. Tällöin tietoa kerätään erityiseen tapahtumatietokantaan tai -lokiin, josta tietoja analysoidaan, joko reaaliaikaisesti, tai myöhemmin erityisten analysointi- ja datamining -ohjelmistojen avulla.

Valvontaa voidaan tehostaa käyttämällä varmennepohjaisia ja biometrisiin ominaisuuksiin perustuvia tunnistamismenetelmiä. Tällöin palveluita käyttävät henkilöt voidaan täysin varmasti ja luotettavasti tunnistaa, jolloin tunnistetietoja yhdistettynä aika- ja paikkatietoihin voidaan käyttää esimerkiksi etsintäkuulutettujen ja kadonneitten henkilöiden jäljittämiseen. Passiiviseen identifiointiin soveltuvat biometriset tunnistamismenetelmät luovat valvonnan kannalta uusia mahdollisuuksia: henkilöitä voidaan tunnistaa esimerkiksi valvontakameran avulla ihmisvirrasta ilman, että henkilöt tietävät tai ymmärtävät tulevansa tunnistetuksi. Teknologian kehittyessä ja tunnistamismenetelmien parantuessa tämä tuo aivan uusia ulottuvuuksia valvonnan kannalta. Tällöin teknologiaa voidaan käyttää edellä mainitulla tavalla etsintäkuulutettujen ja kadonneitten henkilöiden jäljittämiseen, mutta myös esimerkiksi suljetun alueen valvontaan siten, että alueella olevat ja liikkuvat henkilöt tunnistetaan, ja heidän oleskeluoikeutensa tarkistetaan automaattisesti. Järjestelmä antaa hälytyksen, jos alueella havaitaan henkilö, jolla ei ole oikeutta olla alueella. Vastaavasti hälytys annetaan, jos alueella havaitaan henkilö, jota ei pystytä identifioimaan.

Lisäksi, kun biometristä identifiointia käytetään fyysiseen pääsynvalvontaan, syntyy mahdollisuus identifioida myös muita henkilöitä, jotka mahdollisesti haluaisivat pysyä anonyymeinä. Esimerkkinä voidaan kuvata tilanne, jossa elokuvateatterin näytökseen on mahdollisuus ostaa pääsyoikeus (”pääsylippu”) siten, että ostaja pääsee näytökseen kasvontunnistuksen perusteella. Portilla tunnistuksen tekevä laite ilmoittaa, jos kyseinen henkilö voidaan päästää sisään ilman paperista lippua.

Vastaavanlainen tilanne syntyy, jos esimerkiksi kaupan tai ravintolan ylläpitäjä haluaa tunnistaa automaattisesti liikkeeseen tulevat henkilöt, jotta hän voi palvella kanta-asiakkaitaan paremmin, ja toisaalta kieltäytyä palvelemasta ei-toivottuja asiakkaita.

Edellä kuvattu tilanne mahdollistuu kuitenkin vain, jos palveluntarjoajalla on käytössään rekisteri henkilöistä ja heidän biometrisistä ominaisuuksistaan. Kun henkilö rekis-

teröityy kyseiseen rekisteriin, hän antaa yleensä luvan ominaisuutensa perusteella tapahtuvaan tunnistamiseen ja mahdollisesti hyväksyy tunnistamistilanteen mukanaan tuoman veloitusperusteen. Ongelmalliseksi muodostuu tilanne, jossa palveluntarjoaja on aiemmin rekisteröinyt henkilön, mutta henkilöä ei ole asianmukaisesti poistettu rekisteristä esimerkiksi sopimussuhteen päätyttyä, tai jos palveluntarjoaja hankkii tunnistamista varten rekisterin kolmannelta osapuolelta ilman rekisteröityjen henkilöiden suostumusta. Tällöin edellisen elokuva-esimerkin tapauksessa mahdollistuu tilanne, jossa myös perinteisellä paperilipulla näytökseen saapuvat henkilöt voidaan identifioida siten, että he eivät tiedä tulleensa tunnistetuksi.

Edellä kuvatut tilanteet ovat valvonnan, palvelun tarjoajan ja käyttäjän kannalta oivia mahdollisuuksia palveluiden helppokäyttöisyyden ja sujuvuuden kannalta, mutta tuovat selkeitä haasteita yksityisyyden suojan turvaamiseen.

6 Yksityisyyden suojan turvaaminen

Suomen perustuslain (10 §) mukaan [6]:

- "Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla."
- "Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton."
- "Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä."
- "Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana."

Lisäksi henkilötietolaki sääntelee ja toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. [7]

6.1 Anonymiteetti asiointipalveluissa

Henkilön vahva tunnistaminen ja erityisesti passiivisen tunnistamisen mahdollistavat teknologiat tuovat mukanaan yksityisyyden suojan kannalta uusia haasteita. Milloin on esimerkiksi hyväksyttävää vaatia henkilöä tunnistautumaan? Tunnistaminen on luonnollisesti hyväksyttävää, jos asiointiosapuolet tekevät asiointitransaktion, esimerkiksi ostotapahtuman, tilauksen tai maksutapahtuman, johon vaaditaan molempien osapuolten hyväksyntä, ja jonka täytyy olla myös myöhemmin todennettavissa. Tällöin asiointiosapuolet voivat hyväksyä tapahtuman joko perinteisellä tai sähköisellä allekirjoituksella. Tällöin kysymyksessä ei ole pelkkä tunnistaminen, vaan tilanteeseen liittyy yleensä jonkin sopimuksen solmiminen.

Seuraavaksi voidaan pohtia, missä vaiheessa asiointiosapuolet voidaan tunnistaa. Onko esimerkiksi hyväksyttävää vaatia henkilöä tunnistautumaan jo liikkeeseen, ravintolaan tai verkkopalveluun saavuttaessa, ennen kuin varsinainen osto- tai hankintapäätös tehdään, vai onko palveluntarjoajalla velvollisuus antaa asiakkailleen oikeus ”oleilla” liikkeessään anonyymisti vielä asiointi- tai ostopäätöstä tehdessään.

Palveluissa, joissa käsitellään yksilöiden henkilökohtaisia tai arkaluontoisia tietoja, tunnistaminen on luonnollisesti välttämätöntä. Tällaisia palveluja ovat esimerkiksi pankki- ja vakuutuspalvelut, terveydenhuollon palvelut ja tietyt muut viranomaispalvelut. Näissä palveluissa palvelun käyttäjät yleensä myös ymmärtävät tunnistamisen tarpeellisuuden.

Asiointipalvelut päätyvät usein maksun suorittamiseen. Tällöin voidaan kysyä, onko palveluntarjoajalla velvollisuus antaa asiakkailleen mahdollisuus myös anonyymiin maksutapahtumaan, käteiseen tai kolmannen osapuolen varmentamaan maksutransaktioon.

Perinteisessä kasvokkain tapahtuvassa asioinnissa anonymiteetin turvaaminen on ajan myötä muotoutunut varsin mutkattomaksi prosessiksi. Kauppoihin ja liikkeisiin voi saapua anonyymisti ja maksukin voidaan suorittaa käteisellä, jolloin ostettu tuote tai palvelu vaihtaa omistajaa. Kaikki osapuolet pysyvät anonyymeinä ja koko prosessi on helposti ymmärrettävissä. Sähköisessä asioinnissa ongelmaksi muodostuu, että asiointitilanteessa asiointiosapuolet ovat yhteydessä toisiinsa verkon kautta, jolloin yksinkertaisestakin ostotapahtumasta täytyy tehdä sopimus, jotta ostaja voi varmistua ostetun tuotteen tai palvelun toimittamisesta ja myyjä maksun saamisesta. Teknisessä mielessä on mahdollista luoda sähköinen käteinen, tai anonymiteetin takaava kolmannen osapuolen varmentama maksumenetelmä, jota voitaisiin käyttää sähköistä sisältöä myytäessä. Tällöin esimerkiksi palvelusta voisi ostaa musiikkia siten, että musiikin lataaminen mahdollistuu vasta, kun sähköinen käteismaksu on suorittu. Tällöin anonymiteetti säilyisi. Edellä mainittu esimerkki on mahdollinen toteuttaa, mutta haasteeksi nousee järjestelmän luotettavuus: miten voidaan olla esimerkiksi varmoja, että verkkoyhteys ei katkea maksun tapahtumisen jälkeen, ennen kuin ostettu sisältö on toimitettu ostajalle. Perinteisessä kasvokkain tapahtuvassa asioinnissa tällainen ei ole mahdollista, ja näiden tilanteiden estämiseksi sähköisissä palveluissa tehdään yleensä sopimus.

Yleensä palveluntarjoajat ymmärtävät yksilöiden halun pysyä anonyymeina, ja pyrkivät välttämään turhaa palveluihin tapahtuvaa rekisteröintiä. Jos palveluntarjoaja vaatii käyttäjiä tunnistautumaan tai rekisteröitymään, niin palveluntarjoaja ymmärtää yleensä, että palvelu karkottaa osan käyttäjistä ja mahdollisista asiakkaista. Käyttäjillä on mahdollisuus olla saapumatta sellaiseen palveluun, joka vaatii tunnistautumista tai rekisteröintiä.

6.2 Anonymiteetti teknisessä valvonnassa

Teknisessä valvonnassa olisi hyvä määritellä selkeästi, menettääkö tunnistettava henkilö anonymiteettinsä, vai säilyttääkö hän sen. Esimerkkinä voidaan esittää valvontatilanne, jossa yritetään tunnistaa etsintäkuulutettuja henkilöitä ihmisvirrasta. Jos henkilöä ei tunnisteta, hän ei ole etsittyjen listalla, ja hän säilyttää anonymiteettinsä. Jos taas henkilö tunnistetaan, hän on etsintäkuulutettujen listalla, ja hänet voidaan ottaa tilanteessa kiinni.

Tällöin tulee myös arvioida mahdollisen väärintunnistamisen aiheuttamat ongelmat.

6.3 Tunnistustilanteen ymmärtäminen

Edellisissä kappaleissa arvioitiin tunnistamisen tarpeellisuutta ja anonymiteetin säilyttämisen mahdollisuutta eri tilanteissa. Seuraavaksi pohditaan itse tunnistustilannetta.

Teknologian kehittyessä tunnistaminen muuttuu yhä nopeammaksi ja huomaamattomammaksi prosessiksi, ja samalla tunnistamisen luotettavuus kasvaa.

Perinteisessä mielessä tunnistaminen on voinut tapahtua esimerkiksi esittämällä henkilötodistus. Tällöin henkilö ymmärtää tunnistamisen tapahtumisen. Uudenlainen tilanne sen sijaan syntyy, kun biometrisia ominaisuuksia ryhdytään käyttämään henkilöiden tunnistamiseen. Tällöin ongelmia aiheuttaa nimenomaan passiivinen identifioiminen. Aktiivinen autentikointi tai identifiointi ei periaatteessa aiheuta ongelmia: silloin tunnistamisessa vaaditaan edelleenkin henkilöltä aktiivista toimenpidettä, ja henkilö yleensä tällöin myös ymmärtää tulevansa tunnistetuksi. Ymmärryksen parantamista varten tunnistajalle voidaan määritellä erilaisia menettelyvaatimuksia. Voidaan esimerkiksi määritellä, että tunnistettavalle henkilölle tulee tunnistustilanteessa selkeästi ilmaista tunnistustilanteen alkamisesta esimerkiksi kehottamalla: ”katso hetkeksi kameraan tunnistamista varten”. Lisäksi tunnistettaville henkilöille on syytä antaa mahdollisuus perääntyä tilanteesta.

Passiivisessa tunnistamisessa henkilöltä ei vaadita aktiivista toimenpidettä, vaan hänet tunnistetaan ihmisvirrasta automaattisesti. Tällaisessa tilanteessa henkilö ei välttämättä tiedä tai ymmärrä liikkuvansa sellaisella alueella, jossa tunnistamista tapahtuu. Lisäksi varsinaiset tunnistustilanteet saattavat jäädä huomaamatta, jolloin henkilö ei edes tiedä onko hänet tunnistettu. Passiivista tunnistamista käytetään lähinnä teknistä valvontaa varten.

Yksityisyyden suojan kannalta on erittäin tärkeää, että henkilön voidaan olettaa ymmärtävän milloin tunnistus tapahtuu, tai milloin hän liikkuu sellaisella alueella, jossa suoritetaan automaattista passiivista tunnistamista. Tätä tietoisuutta voidaan parantaa määrittelemällä ja merkitsemällä selkeästi ne rajatut alueet, joissa tunnistamista suoritetaan, ja ilmoittamalla selkeästi säilyykö henkilön anonymiteetti tunnistustilanteessa.

Yleisesti ottaen henkilöillä ei liene mitään sitä vastaan, että heidät tunnistetaan myös passiivisesti, jos he ovat antaneet siihen suostumuksensa ennalta tai tunnistamiseen on muutoin hyvät, esimerkiksi yleiseen turvallisuuteen liittyvät perustelut. Edellisestä kohdasta voidaan ajatella esimerkkinä jokin palvelusopimus, jossa palvelun laskutus määräytyy käytön perusteella, ja käyttäjä tunnistetaan käytön havainnointia varten. Jälkimmäisestä kohdasta esimerkkinä voisi olla esimerkiksi julkisten tilojen automaattinen valvonta, ja etsintäkuulutettujen henkilöiden etsintä tuolta alueelta olettaen, että tunnistusmenetelmä tunnistaa vain etsintäkuulutetut henkilöt ja muut säilyttävät tilanteessa anonymiteettinsa. Täytyykö jälkimmäisessä esimerkissä alueella liikkuvia henkilöitä edes informoida?

6.4 Tunnistetietojen hyväksikäyttö

Uudet autentikointimenetelmät eivät sinänsä tuo mitään uutta entiseen verrattuna tunniste- ja käyttötietojen keräämisen ja analysoimisen kannalta silloin, kun käyttäjä ymmärtää tulevansa tunnistetuksi. Tällöin tunniste- ja käyttötietoja voidaan kerätä, analysoida ja käyttää markkinointitarkoituksiin kuten ennenkin, riippuen palvelusopimuksen eh-

doista sekä käyttäjän antamista suostumuksista noudattaen voimassa olevaa oikeudellista sääntelyä.

7 Sääntelyn tarve

Henkilön sähköisen tunnistamisen ja teknisen valvonnan osalta tarvetta sääntelylle on olemassa.

Eri tunnistusteknologiat ja -menetelmät kuitenkin vaikuttavat sääntelytarpeeseen. Käyttäjätunnuksella ja salasanalla sekä vaihtuvilla salasanoilla ja varmenteilla tapahtuva käyttäjän tunnistaminen on nykyisellään varsin toimivaa, eikä vaadi tällä hetkellä muutoksia tai lisäyksiä nykyiseen lainsäädäntöön.

Sen sijaan uudet biometriset tunnistusmenetelmät asettavat vaatimuksia sääntelylle. Pääasiallisena syynä sääntelyn tarpeelle on biometristen ominaisuuksien pysyvyys, peruuttamattomuus ja yksilöivyys. Koska biometrinen ominaisuus on pysyvä osa henkilöä ja henkilö voidaan sen avulla yksilöidä ja tunnistaa, on erityisen tärkeää, että biometristen tietojen muodostamisesta, käsittelystä ja tallentamisesta on säädetty lainsäädännössä. Biometristen ominaisuuksien pysyvyyden lisäksi sääntelyn tarvetta korostaa joidenkin biometristen ominaisuuksien etäluettavuus, mikä mahdollistaa henkilön tunnistamisen ilman, että henkilö edes tietää tulevansa tunnistetuksi.

Sääntelyn tarpeelle voidaan nähdä olevan kaksi pääasiallista syytä:

- yksityiselämän suojan ja yksilön oikeuksien turvaaminen
- kaupallisten palveluiden toimivuuden ja tasavertaisuuden turvaaminen

Edellä mainittujen syiden lisäksi kansalaisten ja muiden yhteiskunnan toimijoiden luottamus uusiin tunnistusmenetelmiin ja niiden turvallisuuteen tulee taata.

7.1 Biometrisen ominaisuuden rekisteröiminen

Biometrinen ominaisuus on pysyvä ja muuttumaton, joten sen yhdistäminen omistajaansa tulee olla rajoitettua. Pahimpana uhkakuvana voidaan nähdä tilanne, jossa rekisteri, joka sisältää henkilötietojen lisäksi tietoja henkilöiden yksilöllisistä ominaisuuksista kuten esimerkiksi kasvonpiirteistä, joutuu vääriin käsiin. Tällöin vilpillinen taho voi käyttää rekisteriä hyväkseen tunnistaessaan esimerkiksi kadulla liikkuvia henkilöitä vaarantaen yksilöiden oikeuden pysyä anonyymeinä. Lisäksi anonymiteetin vaarantuminen voi olla pysyvää ja lopullista, sillä biometrinen ominaisuus on pysyvä osa henkilöä, jota ei voida poistaa tai peruuttaa. Lisäuhka muodostuu siitä, että biometrisen ominaisuuden sähköinen (digitaalinen) tallenne on helposti ja nopeasti kopioitavissa, ja samalla levitettävissä nykyisten tietojenkäsittelylaitteiden ja tietoverkkojen avulla.

Viranomaisten tulee varmistaa, että edellä kuvattu biometristen tunnisteiden väärinkäyttö säädetään rangaistavaksi, ja että väärinkäytön toteuttaminen muodostuu myös tekni-

sesti riittävän vaikeaksi. Samalla ehdotetaan, että säädetty rangaistus on ankarampi kuin mitä henkilörekisteririkoksesta on säädetty. *(Toimenpide-ehdotus 1)*

7.1.1 Henkilötietolain soveltuvuus

Henkilötietolaki sääntelee henkilötietojen keräämistä, tallettamista ja käyttämistä sekä henkilörekisterien ylläpitämistä.

HENKILÖTIETOLAKI (3§)

Laissa tarkoitetaan:

Henkilötiedolla kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Henkilörekisterillä käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta. [7]

Henkilön yksilöivä biometrinen ominaisuus on henkilötietolain mukainen henkilötieto ja henkilöiden tunnistamisessa tarvittava vertailurekisteri on henkilötietolain mukainen henkilörekisteri. Tähän perustuen henkilötietolaki sääntelee jo nykyisellään myös henkilöiden biometristen ominaisuuksien muodostamista, tallentamista ja rekisteröimistä sekä biometristen ominaisuuksien avulla tehtävää henkilön tunnistamista.

Viranomaisten tulee kuitenkin arvioida ja varmistaa henkilötietolain soveltuminen kaikilta osin myös biometrisiin ominaisuuksiin. *(Toimenpide-ehdotus 2)*

7.1.2 Suostumus biometristen ominaisuuksien tallentamiselle

Henkilötietolain biometristen ominaisuuksien tallentamista ja rekisteröintiä koskeva sääntely turvaa yksilön suojaa pääosin riittävästi. Henkilörekisterin pitäjällä on tarkat velvollisuudet tietojen säilyttämisestä ja käsittelystä. Lisäksi rekisterin pitämiselle tulee olla selkeä ja hyväksyttävä käyttötarkoitus, eikä tietoja saa käyttää muuhun kuin ilmoitettuun käyttötarkoitukseen.

Lainsäädännöllä tulisi kuitenkin varmistaa, että yksilöiden biometrisia ominaisuuksia saa tallentaa ainoastaan henkilön suostumuksella. Tämä suostumus tulisi saada rekisteröitävältä henkilöltä aina ennen kuin hänen biometrisiä ominaisuuksiaan taltioidaan. *(Toimenpide-ehdotus 3)*

Tällä lisäyksellä ja henkilötietolain soveltamisella poistuu mahdollisuus (laillisesti) tallentaa ja rekisteröidä henkilöiden biometrisia ominaisuuksia, ja suorittaa niiden avulla henkilöiden tunnistaminen, ilman kyseisten henkilöiden lupaa. Tällöin yksilöiden oikeus anonymiteettiin ei vaarannu. Yksilölle jää kuitenkin mahdollisuus sopia palveluntarjoajan kanssa erikseen esimerkiksi automaattisesti tapahtuvasta tunnistamisesta tietyn palvelun yhteydessä. Ehdotettu lainsäädännön muutos nähdään tämän tutkimustyön tärkeimpänä parannusehdotuksena.

Muuta sääntelyä henkilön anonymiteetin turvaamiseksi ei tarvita. Markkinoiden toimivuus sekä kaupalliset intressit vaativat palveluntarjoajia jatkossakin tarjoamaan asiakkailleen mahdollisuuden asioida anonyymisti. Jos palveluntarjoaja ei mahdollista anonyymiä palvelun käyttöä, on palveluntarjoaja tehnyt siitä tietoisen kaupallisen valinnan. Tällöin asiakkailla on vapaa mahdollisuus olla myös käyttämättä kyseistä palvelua.

Biometristen ominaisuuksien rekisteröimiselle ehdotetaan siis vaadittavan aina rekisteröityjen henkilöiden suostumus. Ainoana poikkeuksena tähän voidaan nähdä viranomaisten ylläpitämät henkilörekisterit, joiden avulla valvotaan ja turvataan yhteiskunnan järjestystä ja turvallisuutta. Lisää tästä aiheesta kappaleessa 7.6 ”Tunnistaminen viranomaistoiminnassa”.

7.1.3 Biometrisen tiedon rekisteröintiä koskeva ilmoitusvelvollisuus

Koska biometrisen tiedon rekisteröiminen ja tallettaminen tulisi pitää mahdollisimman turvattuna, suositellaan rekisterinpitäjälle ilmoitusvelvollisuutta biometristen tietojen tallentamisesta. Tämä ilmoitusvelvollisuus koskisi kaikkia biometrisia tunnisteita rekisteriin taltioivia tahoja. Ilmoitus tehtäisiin tietosuojavaltuutetulle kolmenkymmenen päivän kuluessa rekisterin perustamisesta. *(Toimenpide-ehdotus 4)*

Jo nykyisellään henkilötietolaki velvoittaa rekisterinpitäjän laatimaan rekisteriselosteen, joka on pidettävä jokaisen saatavilla [7]. Biometrisen tiedon tallentamista koskeva ilmoitusvelvollisuus suositellaan toteutettavaksi rekisteriselostetta laajentamalla siten, että selosteessa olisi erillinen ilmoituskohta biometrisestä tiedosta ja sen sisältämistä taltioiduista ominaisuuksista. Ilmoituskohdan tulisi myös yksilöidä käyttötarkoitukset tarkemmin, kuin tämän hetkisessä henkilötietolaissa on vaatimuksena. Jatkossa toimivaltaiset viranomaiset voisivat erikseen valvoa ja seurata biometristen tietojen rekistereitä, tietojen tallentamista ja käsittelyä.

Ehdotus lisää rekisterinpitäjän ja rekisteröidyn henkilön ymmärrystä biometristen tietojen rekisteröinnistä aiheutuvista vaatimuksista ja riskeistä.

7.1.4 Ohjaus ja valvonta

Biometrisen ominaisuuden tallentamista ja rekisteröintiä koskevaa ohjausta ja valvontaa suositellaan lisättäväksi. *(Toimenpide-ehdotus 5)*

Erityisen tärkeää olisi määritellä selkeä viranomaisten laatima ohjeistus sekä kaupallisille toimijoille että palveluiden käyttäjille. Lisäksi palveluntarjoajien tulisi laatia palvelukohtainen viranomaisten laatiman ohjeistuksen perusteella toteutettu käyttäjäohjeistus. Nykyisellään pelkän henkilötietolain soveltaminen aiheuttaa paljon käytännön ongelmia ja epätietoisuutta, sekä palveluntarjoajien että yksityisten henkilöiden keskuudessa.

7.2 Biometrisen ominaisuuden muodostaminen ja tallentaminen

Koska biometrinen ominaisuus on pysyvä ja peruuttamaton osa yksilöä, tulee myös sen muodostamista ja tallentamista rajoittavan tai sallivan sääntelyn olla erityisen tarkkaan harkittua ja suunniteltua.

Teknisesti biometrinen ominaisuus voidaan lukea ja tallentaa käyttäen sellaista yhdensuuntaista matemaattista funktiota (salausta), jossa tallennetusta biometrisesta ominaisuudesta (tallenteesta) ei voida mitenkään laskea tai johtaa alkuperäistä biometristä ominaisuutta. Tällöin biometristen tallenteiden, ja niihin liitettyjen henkilötietojen paljastuminen tai leviäminen, ei vaaranna alkuperäisiä biometrisia ominaisuuksia.

Biometrisen ominaisuuden tallentamisen sääntelyn ydinkohdaksi muodostuu sallitaanko biometristen ominaisuuksien tallentaminen ja rekisteröinti sellaisenaan, vai vaaditaanko tallennettaessa käytettävän sellaista yhdensuuntaista menetelmää, että tallenteesta ei pystytä generoimaan alkuperäistä ominaisuutta.

Seuraavassa on kuvattu kahden eri vaihtoehdon vaikutuksia.

7.2.1 Vaihtoehto 1: Biometrisen tiedon tallennus sellaisenaan kielletty

Vaikka henkilötietolaki sääntelee henkilötietojen ja henkilöiden biometristen ominaisuuksien tallentamista ja rekisteröintiä, on olemassa tarve kieltää yksiselitteisesti biometristen ominaisuuksien tallentaminen siten, että biometrinen ominaisuus on tallennettu sellaisenaan tai siten, että tehdystä tallenteesta pystyttäisiin laskemaan tai johtamaan alkuperäinen biometrinen ominaisuus.

Tällä tarkoitetaan esimerkiksi tilannetta, jossa sormenjäljen tallenteesta voitaisiin generoida alkuperäisen sormenjäljen kanssa riittävän identtinen keinotekoinen kopio alkuperäisestä jäljestä. Vastaavasti esimerkiksi silmän verkkokalvon rakenteen tallenteesta tai kasvojenpiirteiden tallenteesta voitaisiin saada selville henkilön alkuperäiset ominaisuudet ja rakenteet. Sama koskee muitakin biometrisia ominaisuuksia.

Tällaisen tallentamisen yksiselitteisellä kieltämisellä voitaisiin pyrkiä ehkäisemään väärinkäytöksiä ja varautua tilanteisiin, joissa henkilöiden biometrisia ominaisuuksia sisältävä henkilörekisteri joutuisi vilpillisen tahon haltuun. Vaikka henkilötietolaki sääntelee henkilötietojen käsittelyä ja rekisterien ylläpitoa, on kuitenkin mahdollista, että henkilö-

rekisteri päätyy vääriin käsiin esimerkiksi tietomurron yhteydessä, tai vilpillisen rekisterinpitäjän toimesta. Jos henkilörekisterin sisältämät biometristen ominaisuuksien tallenteet on edellä kuvatulla tavalla salattu, yksilöiden alkuperäiset ominaisuudet pysyvät edelleen turvattuna. Tällöin salatulla biometrisella tallenteella ei ole vilpilliselle taholle merkittävää käyttöarvoa.

Ehdotus lisää yksilön suojaa ja luottamusta biometrisiin teknologioihin. Tällä on positiivinen vaikutus biometriaa hyödyntävien palveluiden kehittymiseen ja yleistymiseen Suomessa. Yksityishenkilöiden ei tarvitse pelätä tilannetta, jossa heidän sormenjälkensä, kasvojen piirteensä, kävelytyylinsä tai muu vastaava henkilökohtainen ominaisuus on sellaisenaan tallennettuna eri järjestelmiin ja väärinkäytöstilanteessa mahdollisesti kopioitavissa ja levitettävissä hallitsemattomasti.

Toimenpide-ehdotuksena suositellaan biometrisen ominaisuuden tallentamisen sääntelyä siten, että tallentaminen on sallittua ainoastaan siten, että tallenteesta ei ole mahdollista saada selville alkuperäistä fyysistä ominaisuutta. *(Toimenpide-ehdotus 6)*

7.2.2 Vaihtoehto 2: Biometrisen tiedon tallennus sellaisenaan sallittu rekisteröitävän henkilön suostumuksella

Edellisessä vaihtoehdossa kuvatun ehdottoman kieltämisen vaihtoehdoksi tai rinnalle ehdotetaan toteutettavaksi menettely, jossa biometrisen tiedon tallennus sellaisenaan sallittaisiin rekisteröitävän henkilön suostumuksella. *(Toimenpide-ehdotus 7)*

Tällöin edellisen kappaleen uhkakuvat voivat periaatteessa toteutua, mutta rekisteröitynyt henkilö on tällöin ottanut tietoisen riskin antaessaan erillisen luvan oman henkilökohtaisen piirteen tai ominaisuuden tallentamiselle salaamattomana. Samalla korostetaan yksilön oman tahdon ilmaisun merkitystä.

Vaihtoehto keventää tarvittavia tietojärjestelmiä ja vaihtoehdon tarkoituksena onkin helpottaa palveluiden kehittymistä sekä mahdollistaa jo käytössä olevien palveluiden jatkuminen. Mikäli vaihtoehdon 2 mukainen mahdollisuus sallitaan, on sen seuraukset kuitenkin tutkittava ja arvioitava huolellisesti. Tällöin suositellaan asetettavan lisävaatimuksia rekisterin teknisille ominaisuuksille sekä lisättävän tiedottamisvelvollisuutta viranomaistaholta eri osapuolille, palveluntarjoajilta viranomaisille ja palveluntarjoajilta palvelun käyttäjille.

Lisäksi suositellaan, että suostumuksen tulisi kohdistua vain tiettyyn palveluun, ja että palveluntarjoajan oikeutta siirtää tai jälleenmyydä rekisteritietoja kolmannelle osapuolelle rajoitettaisiin rekisteröitävän henkilön antamasta mahdollisesta suostumuksesta huolimatta.

On huomattava, että tämän kohdan suostumus on laajennus kappaleessa 7.1.2 ”Suostumus biometristen ominaisuuksien tallentamiselle” kuvattuun suostumukseen.

7.2.3 Vaihtoehtojen vertailu

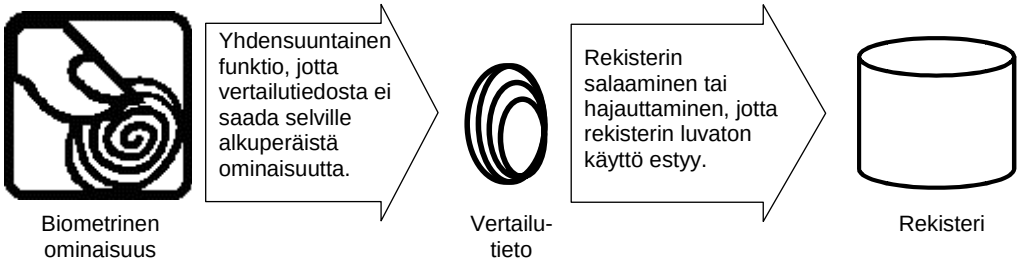
Edellä kuvatut kaksi vaihtoehtoa eivät ole toisensa poissulkevia. Biometrisen ominaisuuden sellaisenaan tallentamisen yksiselitteisellä kieltämisellä voidaan ehkäistä yksilöiden henkilökohtaisten ja pysyvien ominaisuuksien ja piirteiden leviämistä. Jos sellaisenaan tallentaminen halutaan sallia rekisteröitävän henkilön luvalla, palveluntarjoajille annetaan enemmän vapauksia toteuttaa palveluitaan ja lisätään yksilön vastuuta päätöksenteossa. Tämä edellyttää yksilöltä, jonka biometrisiä tietoja rekisteröidään, laajaa ja yksityiskohtaista syy-seuraus -suhteiden tiedostamista ja ymmärtämistä.

Viranomaisten tulisi harkita tarkkaan, tulisiko yksilön suojaa parantaa palveluiden helpomman ja vapaamman kehittymisen kustannuksella, vai tuleeko yksilöille ja palvelutarjoajille antaa mahdollisuus itsenäiseen päätöksentekoon, lisäten samalla heidän vastuuta päätöksenteostaan.

7.3 Oikeudeton biometrinen tunnistaminen

Se, ettei biometrista ominaisuutta tallenneta sellaisenaan, vaan tallennettu vertailutieto on aina generoitu käyttäen yhdensuuntaista matemaattista menetelmää (salausta), ei kuitenkaan estä vertailutiedon käyttämistä henkilöiden tunnistamiseen. Jos biometrista tunnistamista varten perustettu rekisteri päätyy vääriin käsiin, vilpillinen taho voi käyttää rekisteriä henkilöiden oikeudettomaan tunnistamiseen. Vilpillinen taho ei kuitenkaan saa selville henkilöiden biometrisiä ominaisuuksia. Ainoastaan tunnistamista varten tehtävä vertailu on mahdollista. Jos tämäkin halutaan estää, tulee biometristä tunnistusmenetelmiä, -teknologiaa ja niiden prosesseja säännellä. Teknisesti estäminen on mahdollista hajauttamalla tai salaamalla vertailurekisteri.

Seuraavassa on esitetty biometrisen ominaisuuden ja siitä generoidun vertailutiedon tallentaminen vertailurekisteriin, sekä kuvattu käytettävissä olevien teknologisten menetelmien vaikutuksia.



Kuva 13: Biometrisen ominaisuuden tallentaminen

7.3.1 Hajautettu vertailurekisteri

Hajautetulla vertailurekisterillä tarkoitetaan, että tunnistettavat henkilöt pitävät biometrisen tunnistetiedon tallennetta mukanaan esimerkiksi sirukortilla. Tunnistustilanteessa käyttäjä esittää tunnistavalle laitteelle oman biometrisen ominaisuutensa lisäksi hallussaan olevan vertailutiedon. Tällöin tunnistava laite tekee vertailun biometrisen ominaisuuden ja esitetyn vertailutiedon eli tallenteen välillä.

Yhtenä mahdollisuutena nähdään, että sääntely sallisi vain hajautetut ja tunnistettavien henkilöiden hallussa olevat vertailutiedot *(Toimenpide-ehdotus 8)*. Tällöin tunnistettavilla henkilöillä säilyy aina kontrolli tunnistustilanteeseen ja passiivinen tunnistaminen käy mahdottomaksi. Tätä ei kuitenkaan voida ilman lisätutkimuksia suositella, sillä passiivisen (biometrisen) tunnistamisen poissulkeminen rajoittaisi liikaa uusien palveluiden kehittämistä.

Tässä selvityksessä katsotaan hyväksyttäväksi, että palvelun käyttäjä ja palvelun tarjoaja sopivat palvelusta, jossa käytetään passiivista tunnistamista. Tämänkaltaisten palveluiden kehittyminen nähdään myös toivottavana.

7.3.2 Keskitetty vertailurekisteri

Keskitetyn vertailurekisterin vaarana on vertailutietojen leviämisen uhka ja oikeudettoman passiivisen tunnistaminen mahdollistuminen. Vaikka henkilötietolaki kappaleessa 7.1.2 ”Suostumus biometristen ominaisuuksien tallentamiselle” ehdotetun lisäyksen kanssa kieltää biometrisiä tunnisteita sisältävän henkilörekisterin pitämisen, ja siten henkilöiden tunnistamisen ilman rekisteröityjen henkilöiden suostumusta, tulee erikseen arvioida, onko oikeudettoman tunnistamisen uhka niin suuri, että biometristä vertailutietoa sisältävän henkilörekisterin perustamista, ylläpitoa ja tietoturvaa tulisi säädellä erikseen siten, että edellä kuvattu riski pienenee.

Riskiä voidaan pienentää lisäämällä tällaisen rekisterin tietoturvavaatimuksia, asettamalla lisäehtoja rekisterin ylläpidolle, ja laajentamalla rekisterinpitäjän informointivelvollisuutta sekä rekisteröitävien henkilöiden että valvovan viranomaisen suuntaan. Luonnollisesti kaikki rekisterinpitäjille asetettavat lisävaatimukset hidastavat ja vaikeuttavat palveluiden kehittymistä.

Yhtenä selkeänä teknisenä keinona voitaisiin nähdä vaatimus rekisterin salaamisesta siten, että vain rekisterinpitäjä pystyy purkamaan tehdyn salauksen, ja siten näkemään vertailutiedot selväkielisenä. Tällöin mahdollisen tietomurron tapauksessa rekisterin tiedot eivät pääse selväkielisinä vääriin käsiin olettaen, että salauksen purkamiseen tarvittavat tiedot eivät päädy samassa yhteydessä vääriin käsiin. Salauksen teknisenä ratkaisuna voitaisiin käyttää esimerkiksi luotettavaksi todettua julkisen avaimen menetelmää.

Mikäli biometrisiä ominaisuuksia sisältäville henkilörekistereille katsotaan tarpeelliseksi asettaa lisävaatimuksia, suositellaan lisäksi erilaisten teknisten menetelmien, hyväksyttävien prosessien sekä tiedottamisen, ohjeistamisen ja valvonnan tarkkaa lisäselvitystä ja arviointia. (*Toimenpide-ehdotus 9*)

7.4 Tunnistustilanteen kiistämättömyys

Yhtenä ongelmallisena osa-alueena tutkimuksessa nähtiin tunnistustilanteiden kiistämättömyys. Tämä ongelma korostuu jo nykyisissä olemassa olevissa palveluissa, ja lisääntyy passiivisten tunnistusmenetelmien yleistyessä.

Nykyisissä palveluissa ongelma esiintyy lähinnä joidenkin verkkopankkien salasanalistoihin perustuvissa tunnistusmenetelmissä, ja erityisesti tunnistuksen jälkeen tehtävien tapahtumien kiistämättömyydessä. Näissä tilanteissa tapahtumien kiistämättömyys perustuu oletukseen, että käyttäjä on tunnistettu palveluun kirjautuessaan ja sitoutunut samalla kaikkiin palveluistunnon aikana tehtyihin tapahtumiin. Kiistatilanteissa yleensä tutkitaan tekstimuotoisia loki-tiedostoja, jotka pankin järjestelmä on taltioinut. Näiden loki-tiedostojen todenperäisyydestä ei ole olemassa mitään takeita.

Yhtenä suosituksena voidaan pitää, että teknologiaa ja toimintamalleja pyritään ohjaamaan siihen suuntaan ettei tällaisia tilanteita syntyisi. Viranomaisten tulisi pyrkiä vaikuttamaan kehitykseen siten, että palveluntarjoajat huolehtisivat tunnistustilanteen kiistämättömyydestä riittävällä varmuudella. Tässä kehityksessä on syytä ottaa huomioon riittävän pitkät siirtymäkaudet nykysovelluksien osalta. Lisäksi on suositeltavaa ohjata kehitystä siihen suuntaan, että sekä palveluntarjoajat että käyttäjät ymmärtävät tunnistamisen ja tapahtuman hyväksymisen olevan erillisiä, ja toisistaan eroavia tilanteita. (*Toimenpide-ehdotus 10*)

Erityisen tärkeäksi tunnistustilanteen kiistämättömyyden turvaaminen muodostuu niissä palveluissa, joissa tunnistaminen aiheuttaa tietyn velvollisuuden muodostumisen. Esimerkkinä voidaan mainita tilanne, jossa saapuminen suljetulle alueelle aktivoi automaattisen maksutapahtuman. Esimerkki on mahdollinen sekä fyysisessä maailmassa että verkkopalveluissa.

Aktiivisessa tunnistamisessa tunnistamistilanteen kiistämättömyys voidaan turvata helposti käyttäen tunnistamisteknologiana varmenteisiin perustuvaa julkisen avaimen menetelmää, joka on myös laajennettavissa biometrisiin menetelmiin siten, että biometrinen ominaisuus ja sen tarkastaminen vastaa nykyisten menetelmien PIN-koodia, jolla aktivoidaan salaisen avaimen avulla tehtävät toimenpiteet.

7.5 Laatubiotunniste

Yksilön suojan turvaamiseksi ja palveluiden tasavertaisen kehittymisen mahdollistamiseksi yhtenä vaihtoehtona voisi olla yleiskäyttöisen ”laatubiotunnisteen” kehittäminen. (*Toimenpide-ehdotus 11*)

Tällöin nimettäisiin viranomaistaho, joka tuottaisi kansalaisille mahdollisuuden rekisteröidä oma biometrinen ominaisuutensa. Tätä rekisteröityä ominaisuutta kansalaiset voisivat käyttää sekä kaupallisiin että viranomaispalveluihin tunnistautuessaan. Menetelmän tulisi mahdollistaa sekä passiivinen että aktiivinen tunnistaminen.

Viranomainen tarjoaisi turvallisen yleiskäyttöisen biotunnisteen, tunnisteen rekisteröintiin ja käyttämiseen tarvittavat teknologiat ja prosessit, sekä huolehtisi menetelmän toimivuudesta ja turvallisuudesta. Tämä edistäisi palveluiden tasavertaista kehittymistä, lisäisi käyttäjien luottamusta ja turvallisuutta ja edistäisi yksilön suojaa.

Kuvatunlaisen järjestelmän ylläpito toisi luonnollisesti raskaan vastuun rekisteriä ylläpitävälle viranomaiselle. Koko järjestelmä tulisi olla tarkkaan suunniteltu ja valvottu, jotta riittävä turvataso voitaisiin saavuttaa. Järjestelmän kehittämisen mukanaan tuomat kustannukset, vastuut ja velvollisuudet, sekä käytettävät tekniset menetelmät ja sertifiointi- ja toimintamallit suositellaan selvitettäväksi erillisessä tutkimuksessa. Erillisessä tutkimuksessa tulisi myös vertailla viranomaisten tarjoaman yhden keskitetyn rekisterin ja kaupallisesti tarjottavien biotunnistejärjestelmien toteuttamisen välisiä eroja sekä kustannusvaikutuksia yhteiskunnallisesti.

7.5.1 Laatubiotunniste ainoana sallittuna järjestelmänä

Edellä kuvattu järjestelmä antaa palveluntarjoajille mahdollisuuden käyttää viranomaisen tarjoamaa menetelmää palveluidensa käyttäjien tunnistamisessa. Tällöin erillisten palveluntarjoajien ylläpitämien henkilörekisterien tarve pienenee ja samalla pienenee riski henkilötietojen joutumisesta vääriin käsiin.

Jos kuvattu järjestelmä halutaan nähdä ainoana sallittuna vaihtoehtona, edellä kuvatut riskit minimoituvat, mutta samalla rajoitetaan palveluntarjoajien mahdollisuuksia käyttää ja kehittää omia biometrisia tunnistusmenetelmiä. Tämä rajoittaa palveluntarjoajien toimintaa, estää markkinoiden vapaata kehittymistä ja vaikeuttaa uusien innovatiivisten menetelmien kehittymistä.

Yhtenä toteuttamisvaihtoehtona on kuvatun järjestelmän toimiminen tietolähteenä viranomaisten ylläpitämille muille henkilörekistereille (kuten Väestörekisterikeskuksen ylläpitämä väestörekisteri). Tällaista järjestelmää voitaisiin käyttää viranomaispalveluiden lisäksi esim. julkisten tilojen valvontaan, kadonneitten ja etsintäkuulutettujen henkilöiden etsintään sekä esimerkiksi rajavalvontaan. Biometristen tunnisteiden viranomaiskäyttöä käsitellään lisäksi kappaleessa 7.6 ”Tunnistaminen viranomaistoiminnassa”.

7.5.2 Laatubiotunniste rinnakkaisena järjestelmänä

Markkinoiden vapaan toimivuuden ja teknologisen kehityksen turvaamisen kannalta suositeltavampi vaihtoehto on edellä kuvatun laatubiotunniste-järjestelmän tarjoaminen rinnakkaisena vaihtoehtona siten, että sen käyttö perustuu vapaaehtoisuuteen.

Tällöin palveluntarjoajilla säilyy mahdollisuus valita kaupallisten menetelmien ja viranomaisen tarjoaman menetelmän väliltä. Lisäksi säilyy mahdollisuus kehittää täysin oma uusi tunnistusmenetelmä. Valinnan vapauden lisäksi turvataan palveluiden ja teknologioiden kehittyminen markkinavoimien ehdoilla.

7.6 Tunnistaminen viranomaistoiminnassa

Viranomaisilla on olemassa omia tarpeita henkilöiden tunnistamiselle. Tarpeet voidaan jakaa kahteen osa-alueeseen:

- tunnistaminen asiointipalveluissa
- tunnistaminen valvontaa varten

Viranomaisen tulee kehittää molempia tarpeita varten luotettavat, helppokäyttöiset ja kustannuksiltaan kohtuulliset menetelmät. Koska viranomaiset ovat ”pakotettuja” järjestelmien kehittämiseen omia tarpeitaan varten, on suositeltavaa kehittää järjestelmät sellaiseksi, että niiden tuomia ominaisuuksia ja toimintoja voidaan tarjota laajemmin yhteiskunnan käyttöön. Tässä nähdään yksi selkeä peruste kappaleessa 7.5 "Laatubiotunniste” esitetyn kokonaisuuden kehittämiselle. Tällöin järjestelmä olisi monikäyttöisempi, ja järjestelmän kustannukset jakautuisivat käyttöperusteisesti käyttäjien kesken, tarjoten kustannussäästöjä kaikille osapuolille.

7.6.1 Asiointipalvelut

Viranomaiset tarjoavat kansalaisille ja yrityksille useita sellaisia asiointipalveluita, joissa käyttäjän tunnistaminen on kriittisessä asemassa. Yleensä nämä palvelut sisältävät vain yksilöiden tai yhteisöjen omaan käyttöön tarkoitettuja henkilökohtaisia tai arkaluonteisia tietoja, joten palveluntarjoajan tulee olla ehdottoman varma palvelun käyttäjän henkilöllisyydestä. Palvelujen etäkäyttö lisää tarvetta luotettaville sähköisille tunnistusmenetelmille.

On suositeltavaa, että viranomaiset määrittelevät erittäin tarkasti palveluissaan käytettävien tunnistusmenetelmien ominaisuudet ja vaatimukset. Tämä lisää luottamusta viranomaisten palveluihin ja niissä käytettäviin teknisiin menetelmiin, ja edistää palveluiden toteuttamista kustannustehokkaampina ja helppokäyttöisimpinä itsepalvelu- ja etäkäyttöratkaisuina. Tällä on positiivinen vaikutus yhteiskunnan kehittymiselle.

7.6.2 Valvonta

Viranomaisten toimintaan kuluu mm. yleisen turvallisuuden takaaminen, valvonta, rikosten ehkäisy ja rikostutkinta. Passiivisen tunnistamisen mahdollistuminen tuo uusia mahdollisuuksia myös valvonnan toteuttamisen kannalta. Esimerkiksi kadulla kulkevia henkilöitä voidaan tunnistaa automaattisesti.

Jotta automaattinen tunnistaminen olisi mahdollista, tulee viranomaisilla luonnollisesti olla rekisteri henkilötiedoista sekä henkilöiden tunnistamisen mahdollistavista biometrisista ominaisuuksista. Tällaisessa valvonnassa saatetaan kuitenkin helposti loukata yksityisyyden suojaa, joten myös viranomaisten toteuttama valvonta tulisi olla tarkasti säänneltyä. Erityisesti tulisi määritellä erikseen ne tilanteet, joissa kyseinen toiminta on sallittua, ja miten tätä toimintaa tulisi rajoitettaa.

Viranomaisten suorittaman automaattisen passiivisen tunnistamisen osalta toiminnan valvonnan ja tiedottamisen merkitys korostuu. Jotta kansalaisten luottamus viranomaistoimintaan säilyisi, tulee viranomaisten toiminta olla mahdollisimman läpinäkyvää, tarkasti valvottua ja hyvin tiedotettua, myös sähköisen tunnistamisen ja toteutettavan teknisen valvonnan osalta. *(Toimenpide-ehdotus 12)*

8 Kirjallisuusluettelo

1. IEEE Security & Privacy, March/April 2003
2. Tietoverkkojen tietoturva, Esa Kerttula, 1999
3. Applied Cryptography, Bruce Schneier, 1996
4. Cryptography and Network Security, Principles and Practice, William Stallings, 1998
5. Computer Security, Dieter Gollmann, 2000
6. Suomen perustuslaki (731/1999)
7. Henkilötietolaki (523/1999)